Taloushallinnon yrityksen valmistautuminen EU:n uuteen tietosuoja-asetukseen

Oulun yliopisto
Tietojenkäsittelytiede
Pro Gradu –tutkielma
Essi Paso
12.5.2019

Tiivistelmä

Taloushallinnossa käsitellään paljon erilaista henkilötietoa, jota tilitoimiston henkilökunta tarvitsee työssään. Toukokuussa 2018 voimaantullut Euroopan Unionin tietosuoja-asetus velvoittaa yrityksiä ja organisaatioita kiinnittämään enemmän huomiota tietojenkäsittelyyn, kuten tietojen lähettämiseen, vastaanottamiseen ja säilyttämiseen. Tietosuoja-asetus luo myös uusia oikeuksia henkilöille, joiden tietoja käsitellään. Yritysten ja organisaatioiden on luotava kirjallinen dokumentaatio tietojenkäsittelystä, jotta ne pystyvät osoittamaan noudattavansa tietosuoja-asetusta. Tietosuoja-asetuksen noudattaminen on tärkeää, koska asetuksen noudattamattomuudesta voidaan määrätä sakkoja ja sanktioita. On tärkeää tutkia yrityksessä ja sen käytännöissä vaadittavia muutoksia, jotta saadaan selville millaisia vaikutuksia tietosuoja-asetuksella on yritysten toimintaan. Aiempaa kirjallisuutta aiheesta ei vielä ole paljoa, joten tutkimukselle on tarvetta. Aiempi tutkimus käsittelee tietosuoja-asetusta ja sen vaatimuksia, mutta empiirinen tutkimus aihealueesta on erittäin vähäistä.

Tutkimuksen tavoitteena oli luoda selvitys yrityksen nykytilasta tietosuoja-asetuksen vaatimuksiin nähden, sekä selvittää tietosuoja-asetuksen noudattamisen aiheuttamat muutokset yrityksen toiminnassa ja käytännöissä. Muutosten analysointiin hyödynnetään aiempaa kirjallisuutta muutokseen reagoimisesta. Tutkimusmenetelmänä käytetään laadullista tapaustutkimusta. Aineistonkeruumenetelmänä käytetään puolistrukturoitua teemahaastattelua. Tutkimus toteutettiin haastattelemalla toimeksiantajayrityksen henkilökuntaa tietosuoja-asetuksesta ja sen noudattamisesta. Tutkimuksen tuloksena syntyi selvitys yrityksen nykytilasta ja tietosuoja-asetuksen luomista muutoksista yrityksen toiminnassa. Toimeksiantajayritykselle myös toimitettiin suositukset ja ohjeistus tietosuoja-asetuksen noudattamiseen. Tutkimuksen tuloksia voivat myös muut yritykset hyödyntää tietosuoja-asetuksen noudattamisessa ja nykytilansa kartoittamisessa. Jatkotutkimusaiheena on yritysten ja organisaatioiden tietosuoja-asetuksen noudattaminen. Noudattamista voidaan tutkia selvittämällä yritysten luomia ohjeita ja käytäntöjä työntekijöilleen. Tämä tutkimus rajattiin koskemaan vain yhtä tilitoimistoa, joten erilaisia yrityksiä ja niiden tietosuoja-asetuksen noudattamiseen luotuja käytäntöjä vertaamalla voitaisiin luoda yleiset käytännöt erikokoisille ja eri alojen yritykselle tietosuoja-asetuksen noudattamiseen.

Avainsanat
GDPR, Tietosuoja-asetus, Taloushallinto, Tietosuoja

Ohjaaja
FT Tutkijatohtori Mari Karjalainen

Alkusanat

Haluaisin kiittää ohjaajaani Mari Karjalaista hyvästä palautteesta ja ohjauksesta graduni suhteen. Graduprosessi on ollut pitkä ja haastava, mutta mukavan ja ymmärtäväisen ohjaajan ansiosta onnistunut projekti. Haluan myös kiittää ohjaajaani joustavista aikatauluista työnteon ja graduprosessin yhdistämisessä. Lisäksi kiitän tutkielman tilannutta toimeksiantajayritystä ja sen työntekijöitä. Toimeksiantajayrityksen työntekijät olivat aidosti kiinnostuneita aiheesta ja heidän kanssaan yhteistyö onnistui helposti. Graduprosessin viimeistelystä haluan kiittää Anna Rohusta, jonka tietämys tutkielman aiheesta oli erittäin hyödyllistä tutkielman viimeistelyyn. Haluaisin myös kiittää avopuolisoani graduprosessissa tukemisesta.

Essi Paso

Oulu, Toukokuu 12, 2019

Sisällys

1. Johdanto

Teknologian kehityksen myötä yritysten käytössä on yhä enemmän ja enemmän tietoa erilaisissa tietojärjestelmissä ja -varastoissa. Tietoa myös kulkee paljon erilaisten kanavien kautta henkilöltä toiselle. Tietojenkäsittelyyn on olemassa lainsäädäntöä, mutta teknologian kehityksen myötä myös lainsäädännön on kehityttävä. GDPR:n (General Data Protection Regulation) eli Euroopan Unionin (EU) uuden tietosuoja-asetuksen (2016/679) soveltaminen alkoi 25.5.2018, jolloin päättyi kahden vuoden siirtymäaika. Tietosuoja-asetus julkaistiin toukokuussa 2016, jolloin kahden vuoden siirtymäaika alkoi. Siirtymäajalla tarkoitetaan ajanjaksoa, joka yrityksillä oli aikaa käyttää tietosuoja-asetuksen vaatimusten ymmärtämiseen ja käyttöönottoon. Siirtymäaikana yritysten ja organisaatioiden oli varmistettava tietosuoja-asetuksen noudattamisen vaatimat periaatteet toiminnassaan. Periaatteet perustuvat rekisteröidyn oikeuksien turvaamiseen ja tietojenkäsittelyn dokumentointiin. Periaatteet koskevat yrityksen tietosuojaa, tietoturvaa ja tietojenkäsittelyä. Rekisteröidyllä tarkoitetaan henkilöä, jonka tietoja käsitellään. (Talus, Autio, Hänninen, Pihamaa & Kantonen, 2017.) Yritysten mielenkiinnon tietosuoja-asetusta kohtaan on synnyttänyt asetuksen laiminlyönnistä määritelty sakko. Sakko voi olla suuruudeltaan enimmillään 20 miljoonaa euroa tai neljä prosenttia maailmanlaajuisesta liikevaihdosta. (Tikkinen-Piri, Rohunen & Markkula, 2017.)

Tutkielman aihe on ajankohtainen ja tärkeä, koska kuten edellä mainittiin, kaikkien yritysten ja organisaatioiden pitäisi noudattaa uuden tietosuoja-asetuksen periaatteita sekä käytäntöjä toukokuun lopussa 2018. Tietosuoja-asetus koskee kaikkia henkilötietoja käsitteleviä yrityksiä, joten asianosaisia on erittäin paljon. Jo pelkästään Suomessa erikokoisia yrityksiä on 283 563 (Yrittäjät, 2018). Tietosuoja-asetuksen periaatteet ja käytännöt koskevat erikokoisia ja erilaisia yrityksiä eri tavoin. Yritysten on huolehdittava henkilötietojen riskienhallinnasta, jotta mahdolliset riskit voidaan minimoida. Yritysten on myös selvitettävä paljon asioita käytäntöjensä nykytilasta, jotta voidaan tunnistaa muutosta vaativat käytännöt ja toimintatavat. Nykytilan selvityksen jälkeen yrityksen on tunnistettava tietosuoja-asetuksen vaatimat toimenpiteet ja tarvittavat muutokset, jotta yritys voi noudattaa asetuksen vaatimuksia. Tietosuoja-asetuksen noudattamisesta on myös luotava kirjallinen dokumentaatio, jotta yritys voi osoittaa noudattavansa asetusta. (Talus ja muut, 2017.)

Tutkielma käsittelee EU:n uuden tietosuoja-asetuksen vaikutuksia case-yrityksenä olevan tilitoimiston toimintaan. Tilitoimisto toimii myös toimeksiantajayrityksenä tälle tutkielmalle. Toimeksiantajayritys on pieni tilitoimisto ja sitä käsitellään anonyymina tässä tutkielmassa. Toimeksianto sisälsi nykytilan selvityksen tietojenkäsittelystä yrityksessä ja ohjeet tietosuoja-asetuksen noudattamiseen. Tikkinen-Piri, Rohunen ja Markkula (2017) ovat määritelleet 12 yleisen tietosuoja-asetuksen käytännön vaikutusta yritysten toimintaan. Nämä 12 vaikutusta on määritelty vertailemalla Euroopan Unionin tietosuojalainsäädännön keskeistä säädöstä (direktiivi 95/46/EY) EU:n uuteen tietosuoja-asetukseen (2016/679). Tietosuoja-asetus korvasi voimaantullessaan henkilötietodirektiivin (95/46/EY). Ohjeet ja nykytilan selvitys tietosuoja-asetuksen noudattamisesta luotiin edellä mainittujen 12 vaikutuksen ja toimeksiantajayrityksen työntekijöiden haastattelujen vastauksia vertailemalla. Ohjeet toimitettiin raportin muodossa toimeksiantajayritykselle maaliskuussa 2018.

Tutkimuksen tarkoituksena on selvittää EU:n uuden tietosuoja-asetuksen vaatimuksia taloushallinnon alalla toimivan yrityksen työntekijöiden näkökulmasta, joten tutkimusta rajataan koskemaan taloushallintoa ja tilitoimiston toimintaa koskeviin vaatimuksiin ja toimeksiantajayritykseltä kerättyyn aineistoon. Tutkimuksen teoriaosuudessa käsitellään aikaisempaa tutkimuskirjallisuutta aiheesta. Aiempaa tutkimusta kerätään empiirisestä kirjallisuudesta, joka koskee tietosuoja-asetusta ja sen noudattamista. Tutkimuksen yhteydessä toteutetun kirjallisuuskatsauksen perusteella havaittiin, että aikaisempaa tutkimusta aiheesta löytyy vielä melko vähän. Tämä tutkimus eroaa aiemmasta kirjallisuudesta siinä, että tutkimus keskittyy tietosuoja-asetuksen vaatimuksiin ja noudattamiseen taloushallinnon alalla. Suurin osa aiemmasta tutkimuksesta keskittyy käsittelemään tietosuoja-asetuksen vaatimuksia yleisellä tasolla, jolla tarkoitetaan tietosuoja-asetuksen vaatimusten esittelyä.

Tämän tutkielman tutkimuskysymykset ovat;

> Millainen yrityksen nykytila on tietosuoja-asetuksen vaatimuksiin nähden?
>
> Millaisia muutoksia EU:n uuden tietosuoja-asetuksen voimaantulo luo yrityksen toimintaan?

Tutkimuskysymyksiin aineistoa hankitaan yrityksen työntekijöiden haastatteluiden avulla, joilla kerätään työntekijöiden kuvaus yrityksen tietojenkäsittelystä ja siihen liittyvistä käytännöistä. Ensimmäiseen tutkimuskysymykseen vastataan laatimalla työntekijöiden haastattelujen pohjalta kuvaus yrityksen nykytilasta, jota verrataan aiemmassa tutkimuksessa esiteltyihin tietosuoja-asetuksen vaatimuksiin. Nykytilalla tarkoitetaan yrityksen henkilöstön tietämystä tietojenkäsittelystä, tietosuojasta, tietoturvasta ja tietosuoja-asetuksesta. Nykytilan analysointiin viitekehyksenä käytetään Tikkinen-Piri ja muiden (2017) määrittelemää 12 yleisen tietosuoja-asetuksen käytännön vaikutusta yritysten toimintaan ja nykytilaan. Tutkielman tarkoituksena oli luoda ohjeistus ja toimenpiteet toimeksiantajayritykselle tietosuoja-asetuksen noudattamiseen ennen 25.5.2018, jolloin asetus astui voimaan. Ohjeistuksen lisäksi tutkimuksessa on tarkoitus selvittää työntekijöiden haastattelujen perusteella tietosuoja-asetuksen aiheuttamat muutokset yrityksen toiminnassa, joka vastaa toiseen tutkimuskysymykseen. Muutoksilla tarkoitetaan käytäntöjen ja toimintatapojen muutoksia työskentelytavoissa. Toiseen tutkimuskysymykseen vastataan koostamalla yrityksen työntekijöiden mielipiteet ja oletukset tietosuoja-asetuksen luomista muutoksista. Muutosten analysoinnissa viitekehyksenä käytetään Gelderman, Ghijsen ja Brugman (2006) luomaa käsitteellistä mallia EU:n säännösten noudattamiseen. Malliin on koottu neljä oletusta EU:n tarjouskilpailusääntöjen noudattamiseen, joten samoja oletuksia käyetään tietosuoja-asetuksen noudattamisen jäsentelyyn. Tutkimusmenetelmänä käytetään laadullista tapaustutkimusta. Aineistonkeruumenetelmänä käytetään puolistrukturoitua teemahaastattelua, jolla tarkoitetaan etukäteen määriteltyjä haastattelukysymyksiä, joita muokkailtiin ja lisättiin haastattelun edetessä. Haastateltavalla on tällöin vapaus vastata kysymyksiin omin sanoin. Haastattelujen teemat ilmoitettiin haastatelluille etukäteen, kuten teemahaastatteluun kuuluu. (Eskola & Suoranta, 1998, s. 22-64.)

Tutkielma rakentuu seuraavalla tavalla: Tutkielman toisessa luvussa käsitellään taloushallinnon tietojenkäsittelyä ja siihen liittyviä vaatimuksia. Kolmannessa luvussa esitellään tietojenkäsittelyn riskienhallinta, tietosuoja ja tietoturva, koska ne ovat oleellisia tietosuoja-asetuksen näkökulmasta (2016/679). Neljännessä luvussa käydään läpi EU:n uusi tietosuoja-asetus ja sen vaatimukset. Viidennessä luvussa käsitellään käsitteellinen malli EU:n tarjousdirektiivin noudattamiseen tutkimuksen viitekehyksenä.

Kuudennessa luvussa käsitellään aikaisempi tutkimus tietosuoja-asetuksesta. Seitsemännessa luvussa kuvataan empiirisen tutkimuksen tausta ja tutkimusmenetelmät. Luvussa kahdeksan käsitellään haastattelujen tulokset. Yhdeksännessä luvussa käsitellään johtopäätökset ja tutkimustulosten pohdinta aiemman tutkimuksen pohjalta. Viimeisessä eli luvussa kymmenen on vielä yhteenveto koko tutkielmasta.

2. Taloushallinnon tietojenkäsittely

Tämä luku käsittelee tietojenkäsittelyä toimeksiantajayrityksen alalla eli taloushallinnossa. Ensimmäisessä kappaleessa käsitellään digitaalinen taloushallinto yleisesti. Toisessa kappaleessa esitellään taloushallinnon kannalta oleelliset lait ja niiden sisältö. Luvun tarkoituksena on esitellä taloushallinnon tietojenkäsittelyyn liittyvä pohjatieto.

2.1 Digitaalinen taloushallinto

Taloushallinnolla tarkoitetaan organisaation taloudellisten tapahtumien seuraamista raportointitarkoituksiin. Yritysten on lähetettävä erilaisia raportteja ja dokumentteja sidosryhmilleen. (Lahti & Salminen, 2014, s. 16.)

Kuva 1. Taloushallinnon osa-alueita (Lahtinen & Salminen, 2014, s. 16-18).

Kuvassa 1 on esitelty taloushallinnon osa-alueita, joita ovat ostolaskuprosessi, myyntilaskuprosessi, matka- ja kululaskuprosessi, maksuliikenne ja kassanhallinta, käyttöomaisuuskirjanpito, palkkakirjanpitoprosessi, pääkirjanpitoprosessi, raportointiprosessi, arkistointi ja kontrollit (Lahtinen & Salminen, 2014, s. 16-18.)

Taloushallintoa digitalisoidaan koko ajan ja paperin käyttö alalla vähenee. Tietojärjestelmät korvaavat paperilla tehtyjä dokumentteja ja laskenta tapahtuu laskinten sijaan erilaisten ohjelmistojen avulla. Lahti ja Salminen (2014, s. 24) määrittelevät digitaalisen taloushallinnon: ”Digitaalisella taloushallinnolla tarkoitetaan taloushallinnon kaikkien tietovirtojen ja käsittelyvaiheiden automatisointia ja käsittelyä digitaalisessa muodossa. Digitaalisessa taloushallinnossa kaikki kirjanpidon ja sen osaprosessien tapahtumat käsitellään ja ne syntyvät mahdollisimman automaattisesti ilman paperia. Digitaalista taloushallintoa voikin hyvin luonnehtia ja kuvata myös

määritelmällä automaattinen taloushallinto.” Sähköinen ja digitaalinen taloushallinto eivät ole täysin synonyymeja, vaan sähköinen taloushallinto rajataan koskemaan vain sähköisesti tehostettuja taloushallinnon toimintoja (Varanka, Mäkikangas, Hyypiä, Jalonen, & Samppala, 2017, s. 14).

Kuva 2. Talousjohtamisen tehtäviä (Lahti & Salminen, 2014, s. 206-208.)

Digitalisoituminen ja muutokset luovat haasteita taloushallinnon johtamiseen. Kuvassa 2 on esitelty talousjohtamisen tehtäviä, joilla voidaan ehkäistä erilaisten muutosten aiheuttamia riskejä ja haittavaikutuksia. Prosessien johtamisella tarkoitetaan prosessien resursointia ja kontrollointia. Taloushenkilöstön täytyy ymmärtää yrityksen tai organisaation kokonaisprosessit, eikä keskittyä pelkästään talouden prosesseihin. Taloushallinnon kehitystä täytyy seurata, jotta voidaan suunnitella toimivia kehitystoimenpiteitä. Muutoksen johtamisella tarkoitetaan muutoksen läpivientiä oikeaoppisesti ja tehokkaasti. Taloushallinnon tehtävien priorisoinnilla tarkoitetaan sitä, että myös taloustoimintojen on oltava tehokkaita. Resurssit ja ajankäyttö täytyy priorisoida oikein, jotta saadaan tehokkain hyöty niistä irti. Benchmarking tarkoittaa vertailua yrityksen sisällä ja ulkopuolella. Vertailulla varmistetaan kilpailuetu muihin yrityksiin verrattuna tai osastojen välillä yrityksen sisällä. Palvelufunktio tarkoittaa helppokäyttöisten raporttien ja palveluiden tarjoamista asiakkaille. Helppokäyttöisyyteen syntyy haasteita, kun järjestelmät ja prosessit kehittyvät. Kontrolleja voidaan asettaa toiminnan tehostamisen varmistamiseen ja riskien vähentämiseen. Joustavilla organisointitavoilla tarkoitetaan joustavaa suunnittelua, joilla varmistetaan toimiva henkilöstön resursointi ja tietojen saatavuus suunnitelluille henkilöstöryhmille. Joustavan suunnittelun avulla vähennetään ylimääräisiä henkilöresursseja ja tiedon tallentamiseen tarvittavaa tallennuskapasiteettia. (Lahti & Salminen, 2014, s. 206-208.)

2.2 Taloushallinnon tietojenkäsittelyä ohjaavat lait

Fredman (2018) muistuttaa artikkelissaan, että kirjanpitoon ja palkanlaskentaan liittyen tietosuoja-asetus ei estä toisen lain määräyksiä. Palkanlaskenta on yksi yrityksen osakirjanpidoista, mikä tarkoittaa sitä, että kirjanpitolaki koskee myös palkanlaskentaa (Fredman, 2018). Fredman (2018) esittelee artikkelissaan taloushallinnon yritysten toimintaan ja henkilötietojen käsittelyyn tietosuoja-asetuksen lisäksi vaikuttavat lait:

- Kirjanpitolaki (1336/1997),
- Laki yksityisyyden suojasta työelämässä (759/2004) ja
- Henkilötietolaki (523/1999).

Kirjanpitolaki (1336/1997) määrittää kirjanpitoa koskevat lainmukaiset velvoitteet. Kirjanpitoa koskevia velvoitteita laissa ovat esimerkiksi aineistojen säilytysajat ja vaaditut tositteet. Esimerkiksi kirjanpitoaineistoa täytyy säilyttää 10 vuotta (Fredman, 2018).

Laki yksityisyyden suojasta työelämässä (759/2004) kuvaa työnantajan oikeuksia käsitellä työntekijän henkilötietoja. Työnantajan on lain mukaan ilmoitettava työntekijälle henkilötietojen käsittelystä ja niiden keräämisen syystä. Lain yksityisyyden suojasta työelämässä nojalla työnantajalla voi olla myös erityisoikeus käsitellä henkilötietoja, kuten henkilöluottotietoja työnantajalla voi olla oikeus käsitellä, jos kyseessä on erityistä luotettavuutta vaativa työtehtävä. Tietosuojavaltuutetun toimiston (2018) yhteenveto työntekijän henkilötiedoista, joita työnantaja saa käsitellä: ”Työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan tarjoamiin etuuksiin tai jotka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa edes työntekijän suostumuksella. Työnantaja ei siis saa käsitellä mitä tahansa työntekijää koskevia henkilötietoja.” (Tietosuojavaltuutetun toimisto, 2018.)

Henkilötietolaki (523/1999) sisälsi henkilötietojen käsittelyn sääntelyn ennen tietosuojalakia. Hallituksen esitys (HE 9/2018) uudesta tietosuojalaista annettiin 1.3.2018, jonka tarkoitus oli muuttaa henkilötietolakia vastaaman tietosuoja-asetusta (2016/679.) Tietosuojalaki tarkentaa tietosuoja-asetuksessa liikkumavaraa antavia kohtia, kuten esimerkiksi käsittelyn oikeusperustetta, lapsen ikärajaa tietoyhteiskunnan palveluissa, valvontaviranomaisen määritelmää, rangaistussäädöksiä ja sananvapautta.

Andreasson, Koivisto ja Ylipartanen (2016, s. 110-113) esittelevät yritysten toimintaan vaikuttavan myös Arkistolain (831/1994) ja Lain viranomaisen toiminnan julkisuudesta (621/1999). Arkistolaki (831/1994) määrittää ohjeet ja vaatimukset asiakirjojen säilytyksestä ja arkistoinnin järjestämisestä. Arkistonmuodostussuunnitelma määritellään Arkistolain (831/1994) pykälässä kahdeksan. Arkistonmuodostussuunnitelma voi sisältää seuraavia tietoja: organisaation aineistot, aineiston julkisuus tai salassa pidettävyys, aineiston säilytyspaikat, säilytysajat ja rekisterit, joihin tiedot kuuluvat. (Andreasson ja muut, 2016, s. 112-113). Laki viranomaisen toiminnan julkisuudesta (621/1999) 18§ määrittää hyvän tiedonhallintatavan. Laki viranomaisen toiminnan julkisuudesta ohjeistaa myös henkilötietojen luovutuksesta ja julkaisusta. Se määrittää myös joillekkin henkilötiedoille salassapitovelvoitteita, kuten viranomaisten asiakirjoille henkilöiden vuosituloista.

3. Tietosuoja ja tietoturva

Tässä luvussa käsitellään tietosuojaa ja tietoturvaa taloushallinnon yrityksen näkökulmasta. Tietoturva ja tietosuoja liittyvät olennaisesti EU:n uuteen tietosuoja-asetukseen. Myös riskienhallinta on olennainen osa yrityksen tietoturvaa ja tietosuoja-asetuksen vaatimuksia. Tietosuoja-asetus vaatii tietojenkäsittelyyn liittyvien riskien tunnistamisen ja hallinnan. (Talus ja muut, 2017; Tietosuoja-asetus 2016/679.)

3.1 Riskienhallinta tietojenkäsittelyssä

Tietojenkäsittelyssä voi syntyä useita erilaisia riskejä, joihin on varauduttava oikealla tavalla. Tietojenkäsittelyn haavoittuvuuksien tunnistaminen on yksi tärkeä osa riskienhallintaa. Haavoittuvuuksia piilee laitteistossa, ohjelmistossa, verkossa, henkilöstössä, toimipaikassa ja organisaatiossa. Yksityisyyden suojaa koskeva vaikutusten arviointi eli PIA (privacy impact assesment) tarkoittaa tietosuojariskien tunnistamista ja arvioimista. Se sisältää myös tietosuojalainsäädännön noudattamisen seuraamisen, sekä tapoja riskien välttämiseen ja minimointiin. (Wright & De Hert, 2012, s. 7-12.) PIA on yksi tapa suorittaa riskinarviointia ja helpottaa sisäänrakennetun yksityisyyden suojan periaatteen noudattamista (Oetzel & Spiekermann, 2014).

Andreasson ja muut (2016, s. 116-133) määrittelevät riskienhallinnan keskeisimmät tavoitteet yrityksen johdolle: Riskien priorisointi, priorisoitujen riskien hallinta, riskien tunnistaminen, riskienhallinnan johtaminen ja toimintaympäristön muutosten huomiointi. Näiden toimintojen avulla riskit tunnistetaan ajoissa ja niihin pystytään reagoimaan mahdollisimman hyvin. Riskienhallintaa yrityksen toiminnassa avustaa myös erilaisten standardien hankkiminen. Standardien hankkimisella yritys voi todistaa noudattavansa standardin sisältämiä vaatimuksia, koska virallisten standardien hankkimisessa standardin toimittaja vahvistaa standardin noudattamisen yrityksen toiminnassa. Esimerkiksi ISO/IEC 27001 – standardilla yritys määrittelee tietoturvallisuuden hallintapolitiikan standardin vaatimalla tavalla. (Andreasson ja muut, 2016, s. 42-45.)

3.2 Yrityksen tietosuoja

Tietosuoja tarkoittaa: ”Yksityistä henkilöä koskevien tietojen kerääminen, käsittely ja suojaaminen niin, etteivät ulkopuoliset tahot voi käyttää tietoja luvattomasti.” (Järvinen, 2002, s. 451). Järvisen (2002) tietosuojan määritelmä on erittäin käytännönläheinen eli se kuvaa henkilön tietojen käyttämistä vain sallittuihin toimenpiteisiin. Rohunen ja Markkula (2017) määrittelevät tietosuojan koskemaan henkilön oikeuksia hallita häntä koskevaa tietoa. Yksittäisellä henkilöllä on siis oikeus määrittää esimerkiksi hänen tietojaan käsittelevät henkilöt ja tietojen käyttötarkoitus. Tietosuoja koskee siis yksityistä henkilöä, kun taas tietoturva koskee enemmänkin tietojärjestelmiä. Tietosuoja on varmistettava myös tietojärjestelmissä (Männistö, 2017). Tietosuojapolitiikalla tarkoitetaan yrityksen tiedotusta asiakkaille, sekä työntekijöille käyttäjistä kerätyistä tiedoista ja niiden käyttökohteista (Järvinen, 2002, s. 171). Tietosuojaa voidaan kutsua myös yksityisyyden suojaksi (Järvinen, 2002, s. 21). Yksityisyyden suoja eli yksityiselämän suoja, säädetään Suomen perustuslaissa pykälässä kymmenen (731/1999). Siinä määritellään, että jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilön yksityisyys ja hänen yksityisyyttään koskevien tietojen pitäisi olla

turvattuja ja suojattuja. Henkilön yksityisyys on suojattu, kun hänen henkilötietonsa ovat suojattu ja rajattu vain asianosaisten saataville. (Järvinen, 2002, s. 30.)

Henkilötiedolla tarkoitetaan kaikkia tunnistetietoja, joilla luonnollinen henkilö tunnistetaan tai voidaan tunnistaa. Esimerkiksi nimi, osoite, terveystiedot, sähköpostiosoite ja henkilötunnus ovat henkilötietoja. Henkilötiedon käsittelyllä tarkoitetaan henkilötiedon tallentamista, säilyttämisestä, keräämistä, siirtämistä ja muokkaamista. (Tietosuoja-asetus 2016/679.) Henkilötietolaki (523/1999) määritteli henkilötietojen käsittelyn vaatimukset ennen kuin se kumottiin Tietosuojalailla (1050/2018), joka tuli voimaan 1.1.2019. Henkilötietolain (523/1999) nojalla henkilötietojen käsittelyn tuli olla suunniteltua ja käyttötarkoitussidonnaista. Käyttötarkoitussidonnaisuudella tarkoitetaan sitä, että tietoja käsitellään vain ennalta määrättyä tehtävää varten, johon rekisteröity on suostunut. Henkilötietolain mukaan henkilötietoja saa käsitellä vain esimerkiksi rekisteröidyn yksiselitteisellä suostumuksella tai rekisteröidyn toimeksiannosta, kuten myös Tietosuojalaissa määritellään (1050/2018). Rekisteröidyllä tarkoitetaan henkilöä, jonka tietoja käsitellään. Rekisteröidyllä tarkoitetaan tarkemmin tietosuoja-asetuksessa; ”..luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella..” (2016/679.) Henkilötietolaki (523/1999) määrää myös, että henkilötiedot on suojattava asiattomalta ja väärältä käytöltä.

Tietosuojan noudattamista yrityksessä voidaan seurata lokitietojen avulla, koska niistä voidaan tunnistaa työntekijöiden asiattomia toimintoja. Lokitietojen tallentaminen on hyödyllinen tapa seurata asiattomia tietojen urkinta tapahtumia. Automatisoidut lokijärjestelmät tallentavat käyttäjien avaamat henkilötiedot, jolloin käyttäjän asiattomasta toiminnasta jää merkintä lokitiedostoon. Lokitiedostosta voidaan myös seurata mahdollisesti hälyttäviä toimintoja erilaisten raporttien avulla. Lokitiedot on suojattava hyvin, jotta kukaan ei pääse muokkaamaan niitä ilman perusteltuja oikeuksia. (Andreasson ja muut, 2016, s. 142-143.) Jokaisella yrityksen työntekijällä täytyy olla omat käyttäjätunnukset, jotta lokitiedot tallentuvat oikein. Yrityksen on myös tiedotettava työntekijöitään lokitietojen keruusta ja ohjeistettava tietojenkäsittelyssä. (Andreasson ja muut, 2016, s. 71-73.)

3.3 Yrityksen tietoturva

Tietoturvalla tarkoitetaan tietoon liittyvien tavoitteiden noudattamista: tiedon luottamuksellisuuden, eheyden, saatavuuden, todentamisen, pääsynvalvonnan ja kiistämättömyyden. Luottamuksellisuudella tarkoitetaan tiedon käsittelyn rajaamista vain tietoon oikeutetuille henkilöille. Eheydellä tarkoitetaan tiedon säilymistä ilman hyväksymättömiä muutoksia. ”Esimerkiksi yrityksen taloustiedot ja turvajärjestelmiin liittyvät lokitiedostot on arkistoitava niin, ettei kukaan pysty muuttamaan niitä myöhemmin.” (Järvinen, 2002, s. 24.) Saatavuudella tarkoitetaan sitä että tieto on saatavilla yrityksen toimintaan sopivana aikana. Todentamisella tarkoitetaan käyttäjän tunnistamista, joka voidaan hoitaa auktorisoinnilla eli käyttäjätunnuksella ja salasanalla. Pääsynvalvonnalla tarkoitetaan jatkoa todentamiselle. Kun käyttäjä on todennettu, järjestelmä tarkistaa käyttäjän oikeudet järjestelmään. Lokitietojen tallentaminen on myös osa pääsynvalvontaa, koska lokitiedot syntyvät tässä vaiheessa. Kiistämättömyys tarkoittaa erilaisten toimintojen varmistamista. Sillä tarkoitetaan esimerkiksi tilannetta, jossa asiakkaan on saatava tosite asioinnista. Tositteen on sisällettävä järjestelmän tulostamat aikaleimat asiakkaan tekemästä tilauksesta ja sen vaiheista, jotta mahdollinen

ongelmatilanne olisi helppo ja selkeä selvittää ilman arvelua tapahtumasta ja sen sisällöstä. (Järvinen, 2002, s. 24-28.)

Järvinen (2002) kuvaa kirjassaan yrityksen tietoturvan kannalta huomioon otettavat tietojenkäsittelyn elementit: tietokoneet, netinkäyttö, sähköposti, etätyö ja yleiset ohjeet. ”Tietokoneet” -elementti sisältää ohjeet tietokoneen käyttöön noudattaen tietoturvallisia tapoja. Netinkäytöllä tarkoitetaan työntekijöiden kanssa sovittuja käytäntöjä internetin käyttöön. Sähköpostin käyttöä täytyy myös ohjeistaa. Etätyöskentely on noussut suosioon teknologian kehityksen myötä, joten työntekijöiden on huolehdittava kotioloihin yhtä hyvä tietoturva kuin työpaikalla. (Järvinen, 2002, s. 117-120.)

Järvinen (2002, s. 120) suosittelee kirjassaan yrityksiä ohjeistamaan työntekijöitään huolella etätyöskentelyssä, koska kotioloissa on piileviä riskejä, joita työntekijä ei välttämättä huomaa itse. Työntekijöitä on ohjeistettava esimerkiksi tietoliikenneyhteyksissä, muiden asukkaiden huomioinnissa ja tietokoneen säilyttämisessä. Työntekijöiden valvonta on myös haastavaa etätyötä tekeville. (Järvinen, 2002, s. 131.) Yrityksen työntekijöille luotava ohje voi olla esimerkiksi seuraavanlainen kunnanhallituksille ja kuntayhtymille tarjottu ohje: ”Ammatillisiin tarkoituksiin käytettävien ohjelmistojen ja tietojen suojauksen on oltava etätyössä lähtökohtaisesti samaa tasoa kuin työnantajan tiloissa työskentelevillä. Etäyhteyden suojaus saattaa lisäksi edellyttää erityisjärjestelyjä. Jos etätyöhön käytettävää tietokonetta saa käyttää myös omiin tarkoituksiin, työnantajan ja työntekijän on syytä sopia pelisäännöistä muun kuin työkäytön osalta sekä arvioida muun käytön riskit tietosuojaukselle. Tietoturvaa koskevat säännökset ovat myös lähtökohtaisesti samat, joita sovelletaan työnantajan tiloissa työskenteleviin.” (Kuntatyönantajat, 2005).

Sähköposti on erittäin suosittu viestintämuoto yritysmaailmassa. Tietomäärän ja sen monipuolisuuden vuoksi sähköpostin luotettavuus on taattava. Matkassa lähettäjältä saajalle on useampi piste, jossa viesti voi päätyä vääriin käsiin. Vaikka sähköposti voi joutua vääriin käsiin, tekstiviestit, faksit tai kirjeet eivät ole turvallisempia. (Järvinen, 2002, s. 217.) Sähköpostin korvaamiseen on olemassa erilaisia asiakaspalvelujärjestelmiä (Anttila, 2018). Tietosuoja-asetus (2016/679) ei erikseen ota kantaa sähköpostin käyttämiseen, mutta palvelun tarjoamisen turvallisuus ja luotettavuus on varmistettava. Anttilan (2018) artikkelissa todetaan, että varsinkin arkaluontoisten tietojen lähettämistä sähköpostilla on harkittava tarkkaan. Taloushallintoliiton ohjeistuksen mukaan palkkalaskemia voi edelleen tietosuoja-asetuksen voimaantulon jälkeen lähettää suojaamattomalla sähköpostilla, mikäli asiakas ei erikseen vaadi muuta tapaa. (Taloushallintoliitto, 2018.) Fredman (2017) suosittelee palkanlaskennan aineiston lähetyksen ja vastaanoton keskittämistä nimetylle vastuuhenkilölle. Työntekijöille on myös tehtävä ohjeistus tietojen luovutus- ja keruutavoista.

Taloushallinnon alalla tietoturvaa voidaan edesauttaa käyttöoikeuksien rajaamisella, henkilöstön koulutuksella ja salassapitosopimuksilla, myös tietojärjestelmien päivityksillä on osuutensa tietoturvan ylläpidossa (Saario, 2018). Taloushallinnon alalla ohjelmistoja on usein tilattu eri toimittajilta. Taloushallinnon alalla tietoturva on huomioitava myös kaikkien järjestelmien toimittajien osalta. Toimittajien tietoturvasta ja sen toteuttamisesta on oltava kirjallinen dokumentointi. (Männistö, 2017.) Seuraavissa kappaleissa käsitellään yrityksen tietopääoma ja tietoturvapolitiikka. Tietopääoman suojaaminen on myös osa yrityksen tietoturvaa, koska se turvaa yrityksen toiminnan jatkuvuutta (Saario, 2018). Tietoturvapolitiikka sisältää yleiset ohjeet tietokoneiden käyttöön, netin käyttöön ja muut yleiset ohjeistukset.

3.3.1 Tietopääoma ja sen suojaaminen

Tietopääoman määrittely on haastavaa, koska tiedon arvokkuus on kontekstisidonnaista, eli tiedon arvokkuus riippuu yrityksestä. Yrityksen on itse tunnistettava toiminnassaan arvokas tieto ja sen käyttötarkoitus. (Käpylä & Salonius, 2013, s. 76.) Tietopääoman tunnistaminen ja arvioiminen voi olla hankala prosessi, koska tiedon arvo ei ole yksiselitteistä (Käpylä & Salonius, 2013, s. 45-46). ”Yrityksen tietopääoman suojaaminen lähtee siitä, että yritys tunnistaa suojattavan tiedon ja suojaa sen tarkoituksenmukaisesti” (Saario, 2018). Yritysten on tiedostettava, että yritysvakoilua tapahtuu erilaisiin yrityksiin eri aloilla. Suojattavan tiedon tunnistaminen on tärkeää, jotta voidaan järjestää tiedolle sopiva suojausmekanismi. (Saario, 2018.) Tietopääoma voidaan jakaa neljään osa-alueeseen: inhimilliseen pääomaan, suhdepääomaan, rakennepääomaan ja sosiaaliseen pääomaan. Inhimillinen pääoma on yksilön omistamaa tietoa. Suhdepääomaa ovat arvokkaat suhteet ja imago. Rakennepääomaa on yrityksen rakennetta kuvaava tieto. Sosiaalista pääomaa ovat luottamus ja kommunikaatio. Sosiaalinen pääoma sitoo inhimillisen pääoman, rakennepääoman ja suhdepääoman yhteen. (Käpylä & Salonius, 2013, s. 42-43.)

Henkilöstön tietosuoja- ja tietoturvaosaamisen ylläpito pienentää tiedon väärinkäytön riskejä, koska usein väärinkäyttö voi johtua myös työntekijän osaamattomuudesta. Henkilökunnan koulutus on siis tärkeä osa yrityksen tietosuojan ja tietoturvan noudattamista. (Andreasson ja muut, 2016, s. 100-105.) Henkilöstön tietämykseen liittyvät myös salassapitosopimukset, joiden tarkoitus on estää tiedon levittämistä ja taata työntekijän salassapitovelvollisuus myös työsuhteen päättyessä. (Järvinen, 2002, s.112).

3.3.2 Tietoturvapolitiikka

Järvinen (2002) määrittelee kirjassaan tietoturvapolitiikan sisällön, joka on yrityksen työntekijöiden ja henkilökunnan ohje tietoturvan noudattamiseen. Tietoturvapolitiikka sisältää toimintaohjeet, politiikat ja koulutuksen. Toimintaohjeet sisältävät poikkeustilanteisiin reagoimisen sekä ohjeistuksen muihin harvemmin tapahtuviin tietokoneisiin tai ohjelmistoihin liittyviin tapahtumin, kuten varmuuskopiointiin. Politiikat koskevat ohjelmistojen käyttöä, esimerkiksi sähköpostilla lähetettäviin asioihin voi olla yrityksen ohjeistuksessa rajoituksia, kuten mitä saa lähettää sähköpostilla ja mitä ei. (Järvinen, 2002, s. 116.)

VAHTI-ohje, Johdon tietoturvaopas (2011, s. 29-30) sisältää esimerkin tietoturvapolitiikasta, joka on julkaistu myös VAHTI Tietoturvallisuudella tuloksia – ohjeessa (2007, s. 29-30). Ohje sisältää kappaleet;

1. Johdanto
2. Tietoturvapolitiikan tavoite
3. Tietoturvatoimintaa ohjaavat tekijät
4. Tietoriskien hallinta
5. Tietoturvallisuuden merkitys organisaatiolle
6. Turvatoimien priorisointi
7. Tietoturvallisuuden hallintajärjestelmä

8. Tietoturvavastuut
9. Tietoturvakoulutus ja -ohjeet
10. Tietoturvallisuudesta tiedottaminen
11. Tietoturvallisuuden toteutumisen valvonta
12. Toiminta poikkeustilanteissa ja – oloissa

Ensimmäinen kappale sisältää johdon sitoutumisen osoituksen ja määrittelyt tietoturvasta. Seuraava kappale sisältää tietoturvallisuuden käsitteet, määritelmät, tavoitteet ja merkityksen. Suojattavien kohteiden tunnistaminen on myös ohjeistettava. Kolmannessa kappaleessa on toimialakohtaiset velvoitteet, ohjeet ja lait, jotka vaikuttavat tietoturvallisuuden noudattamiseen. Neljännessä kappaleessa käydään läpi uhkien tunnistus, riskien hallinta ja vaikutusanalyysi. Viides kappale on yleiskuvaus organisaation tietoturvallisuuden keskeisistä periaatteista ja niiden toteuttamisen toimintatavoista. Kuudennessa kappaleessa priorisoidaan turvattavia kohteita, jos sille on perustellusti tarvetta. Seitsemännessä kappaleessa käydään läpi tietoturvallisuuden hallintajärjestelmä. Kahdeksannessa kappaleessa kuvataan organisaation tietoturvavastuut ja organisaation yhteistyökumppaneiden vastuut. Yhteistyökumppaneilla tarkoitetaan asiakkaita ja muita sidosryhmiä. Yhdeksännessä kappaleessa kuvataan organisaation tietoturvaohjeistus, koulutus ja perehdyttäminen. Perehdyttäminen on työntekijöiden kouluttamista tietoturvan periaatteista ja käytännöistä. Kappaleessa 10 kuvataan kuinka tietoturvallisuudesta tiedotetaan yrityksen sisällä. Ohjeistus voi muuttua tai joihinkin kohtiin voi tulla tarkennuksia, joten viestintä on tärkeää. Kappaleessa 11 selvennetään tietoturvallisuuden valvonta- ja raportointitavat. Kappaleessa 12 ohjeistetaan toiminta poikkeamatilanteissa. (VAHTI 2007, s. 29-30; VAHTI 2011, s. 85.)

4. GDPR eli EU:n uusi tietosuoja-asetus

EU:n uusi tietosuoja-asetus luo yrityksille uusia vaatimuksia, jotka käydään läpi tässä luvussa. Monet vaatimuksista tulevat vielä tarkentumaan tulevaisuudessa. Tikkinen-Piri ja muut (2017) ovat määritelleet 12 vaatimusta tietosuoja-asetuksen noudattamiseen yritysten toiminnassa. Vaatimukset liittyvät yrityksen henkilötietojen käsittelyyn, tietoturvaan ja tietosuojaan, sekä dokumentaatioon tietojenkäsittelystä.

Tikkinen-Piri ja muiden (2017) määrittelemät tietosuoja-asetuksen noudattamisen käytännön vaikutukset ovat;

1. Tietotarpeiden ja tietojen käyttötarkoitusten määrittäminen,
2. Tietojen käsittelyn edellytykset kansainvälisissä yhteyksissä,
3. Rakennetaan yksityisyyttä sisäänrakennetulla ja oletusarvoisella tietosuojalla,
4. Osoitetaan GDPR vaatimusten täyttäminen,
5. Kehitetään prosesseja tietoturvaloukkausten käsittelyä varten,
6. Sanktiot asetuksen noudattamattomuudesta,
7. Määritetään tietosuojavastaava,
8. Tarjotaan tietoa rekisteröidyille,
9. Suostumuksen hankkiminen henkilötietojen käytöstä,
10. Varmistetaan yksilöiden oikeus tulla unohdetuksi,
11. Varmistetaan yksilöiden oikeus tiedon siirtämiseen ja
12. Dokumentaation ylläpito.

Edellä mainittuja 12 vaatimusta käytetään tutkielman viitekehyksenä jäsentämään yrityksen nykytilan mahdollisia puutteita tietosuoja-asetuksen noudattamisessa. Noudattamisella tarkoitetaan tässä tutkielmassa tietosuoja-asetuksen vaatimien toimintatapojen mukaisia käytäntöjä, sekä käytäntöjen dokumentointia ja ohjeistusta yrityksen toiminnassa. Viitekehyksen tarkoituksena on toimia eksplisiittisesti määriteltynä näkökulmana, jonka avulla havaintoja tarkastellaan (Alasuutari, 2011, s. 60). Tiedon tarjoaminen rekisteröidylle ja suostumuksen hankkimien henkilötietojen käytöstä poikkeavat viitekehyksestä. Viitekehyksestä poiketen tiedon tarjoaminen rekisteröidylle (vaatimus 8) on käsitelty kappaleessa 4.8 Henkilötietojen käsittelijä. Tilitoimisto toimii henkilötietojen käsittelijänä, joten tiedon tarjoaminen pohjautuu sopimukseen asiakasyrityksen ja tilitoimiston välillä. Suostumus (vaatimus 9) jätetään tässä tutkielmassa käsittelemättä. Suostumuksen sijasta tässä tutkimuksessa käsitellään tietojenkäsittelysopimusta, jolla tarkoitetaan asiakasyrityksen määrittelemää ohjeistusta ja lupaa tilitoimistolle käsitellä tarvittavia tietoja. Tietojenkäsittelysopimus käsitellään

kappaleessa 4.8. Tietojenkäsittelysopimus sisällytetään toimeksiantoon asiakasyrityksen ja tilitoimiston välillä (Taloushallintoliitto, 2018). Yksilön oikeus tulla unohdetuksi (vaatimus 10) ja oikeus tiedon siirtämiseen (vaatimus 11) on käsitelty kappaleessa 4.9 Rekisteröidyn/Rekisterinpitäjän oikeudet ja velvollisuudet. Henkilötietojen käsittelijän on huomioitava kaikki tietosuoja-asetuksessa määritellyt oikeudet, jotta se pystyy toteuttamaan tai tietää syyn olla toteuttamatta niitä. Tikkinen-Piri ja muiden (2017) määrittelemät 12 vaatimusta käsitellään tässä tutkielmassa 10 vaatimuksena, jotka soveltuvat hyvin määrittämään tutkimuksen kohteeksi valitun yrityksen nykytilan mahdollisia puutteita, koska niiden kautta esitetään tietosuoja-asetuksen muutokset ja vaikutukset yrityksille.

Tietosuoja-asetuksen (2016/679) *rekisterinpitäjällä* tarkoitetaan;

”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot..”

Tietosuoja-asetuksen (2016/679) *henkilötiedon käsittelijällä* tarkoitetaan;

”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.”

Tietosuoja-asetuksen (2016/679) *henkilötiedolla* tarkoitetaan;

”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön – liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.”

Tietosuoja-asetuksen (2016/679) *erityisiä henkilötietoryhmiä eli arkaluonteisia tietoja koskeva käsittely* tarkoittaa;

”Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä.”

Tietosuoja-asetuksen (2016/679) *rekisteröidyllä* tarkoitetaan tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä, jonka henkilötietoihin käsittely kohdistuu.

4.1 Tietotarpeiden määrittäminen

Tietosuoja-asetuksen (2016/679) viides artikla määrittää henkilötietojen säilytykselle erilaisia vaatimuksia. Henkilötietoja on käsiteltävä oikein ja rekisteröidyn kannalta läpinäkyvästi. Tämä tarkoittaa sitä, että rekisteröidyllä on oikeus tietää hänestä säilytettävistä tiedoista. Rekisteröidyn täytyy myös tietää seurauksista, jos hän kieltäytyy toimittamasta haluttuja tietoja.

Tietosuoja-asetuksen (2016/679) viides artikla sisältää myös tiedon minimoinnin periaatteen, jolla tarkoitetaan henkilötietojen keräämistä ja säilyttämistä vain määriteltyä tarpeellisuutta varten. Henkilötietojen kerääminen ja säilytys on siis

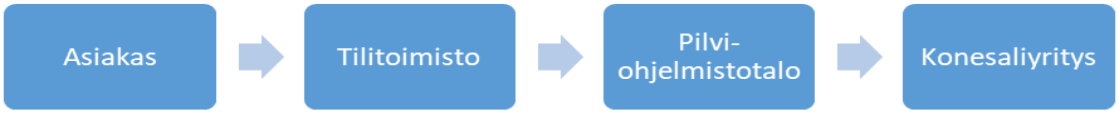
tarpeellista vain, jos tietojenkäsittelyn toteuttaminen sitä vaatii. Tietosuoja-asetuksen 15 artikla kehottaa henkilötietojen säilytysajan suunnittelua. Monia henkilötietoja koskevat arkistoinnin säilytysajat. Suomen kuntaliitto (2009) on antanut suosituksensa kunnallisten asiakirjojen säilytyksestä taloushallinnon tehtäväalalta. Tietosuoja-asetuksen (2016/679) mukaan henkilötiedot on myös nopeasti poistettava tai oikaistava, mikäli niissä esiintyy virheitä.

Tikkinen-Piri ja muut (2017) määrittävät artikkelissaan tietotarpeiden määrittämisen ja käytön koskevan yrityksen toiminnan kannalta olennaisia tietoja. Yrityksen on siis luvallista käyttää vain tietoja, joita ilman yritystoiminta on mahdotonta. Näiden tietojen keruusta täytyy ilmoittaa asiakkaalle syyt ja hankkia heidän suostumuksensa. Tietosuoja-asetus (2016/679) vaatii tietojenkäsittelyn oikeusperusteen määrittämisen eli tietojenkäsittelyn lainmukaisuuden määritelmän. Oikeusperuste on ilmoitettava rekisteröidylle, kun tietoja kerätään.

4.2 Tietojenkäsittelyn edellytykset kansainvälisissä yhteyksissä

Tietosuoja-asetus (2016/679) määrittää, että jos henkilötietoja siirretään Euroopan Unionin ulkopuolelle, asianmukainen ja turvallinen tiedonkäsittely tulee varmistaa kohdemaassa. Myös henkilötietolaki (523/1999) vaatii varmistamaan tietosuojan riittävän tason kohdemaassa. ”Tietosuojan tason riittävyys on arvioitava ottaen huomioon tietojen luonne, suunnitellun käsittelyn tarkoitus ja kestoaika, alkuperämaa ja lopullinen kohde, asianomaisessa maassa voimassa olevat yleiset ja alakohtaiset oikeussäännöt sekä käytännesäännöt ja noudatettavat turvatoimet.” (Henkilötietolaki 523/1999).

Nykyaikana pilvipalveluiden käyttö on yleistynyt. Pilvipalveluilla tarkoitetaan ohjelmistoja internetin välityksellä, joita pilvipalvelun tarjoaja tarjoaa. Pilvipalveluiden tarjoaja voi sijaita erissä maassa kuin ostaja. Tietoturva on yksi pilvipalveluiden haasteista. (Armbrust ja muut, 2010.) Yritysten on varmistettava, että pilvipalveluiden tarjoajat noudattavat tietosuoja-asetusta.



Kuva 3. Asiakkaan alihankkijaketju (Fredman, 2018.)

Kuvassa 3 on esitelty asiakkaan alihankkijaketjua, jonka perusteella asiakas on tilitoimiston kautta vastuussa myös ohjelmistotalon ja konesaliyrityksen tietojenkäsittelystä. Asiakkaan on siis tehtävä tilitoimiston kanssa sopimus, jossa hyväksytään tietojen jakaminen ohjelmistotalolle ja siitä eteenpäin. Täytyy muistaa, että myös tietojen näkeminen lasketaan käsittelyksi. (Fredman, 2018.)

4.3 Sisäänrakennettu ja oletusarvoinen tietosuoja

Talus ja muut (2017) määrittelevät tietosuojaperiaatteiksi;

- *käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys*
- *käyttötarkoitussidonnaisuus*
- *tietojen minimointi*
- *tietojen täsmällisyys*
- *tietojen säilytyksen rajoittaminen*
- *tietojen eheys ja luottamuksellisuus*
- *rekisterinpitäjän osoitusvelvollisuus.*

Sisäänrakennetun tietosuojan periaatteen noudattamiseksi edellä mainitut periaatteet on otettava osaksi henkilötietojen käsittelyä sisältäviin toimintoihin (Talus ja muut, 2017).

Hoepman (2014) toteaa artikkelissaan tietosuojan suunnittelun olevan tärkeä sisäänrakennetun ja oletusarvoisen tietosuojan kannalta. Hän esittää artikkelissaan kahdeksan tietosuojastrategiaa; minimointi, piilotus, erotus, koonti, ilmoittaminen, hallinta, toteutus ja osoittaminen. Minimoinnilla (minimise) tarkoitetaan, ettei tietoa kerätä ilman syytä. Piilotuksella (hide) tarkoitetaan sitä, etteivät kaikki järjestelmän tiedot ole jokaisen käyttäjän saatavilla tai käytettävissä. Erottamisella (separate) tarkoitetaan henkilön tietojen käsittelyn jakamista eri varastoihin, jolloin henkilön profiilin luonti vaikeutuu. Yhdistämisellä (aggregate) tarkoitetaan henkilötietojen keräämistä ja yhdistämistä, säilyttämällä mahdollisimman vähän yksityiskohtia kerätyistä henkilötiedoista. (Hoepman, 2014.) Ilmoittamisella (inform) tarkoitetaan tietojen läpinäkyvyyttä eli rekisteröity saa aina tiedon, kun hänen tietojaan käsitellään. Rekisteröidyn tulisi tietää, mitä, miten ja miksi tietoja käsitellään. Hallinnalla (control) tarkoitetaan rekisteröidyn oikeutta nähdä, päivittää ja mahdollisuuksien rajoissa poistaa häntä koskevat tiedot. Toteuttamisella (enforce) tarkoitetaan lakisääteisen tietosuojapolitiikan noudattamista yrityksessä. Osoittamisella (demonstrate) tarkoitetaan tietosuojapolitiikan noudattamisen osoittamista eli noudattamisen todistamista. Osoittamisen strategia tarkoittaa samaa kuin EU:n uuden tietosuoja-asetuksen osoitusvelvollisuus. Nämä kahdeksan strategiaa perustuvat tietosuojalainsäädäntöön, OECD:n ohjeisiin ja ISO 29100 periaatteisiin. (Hoepman, 2014.) Danezis ja muut (2015) selittävät erityisesti neljän kahdeksasta strategiasta nojaavan EU:n uuteen tietosuoja-asetukseen eli GDPR; ilmoittamisen, hallinnan, toteutuksen ja osoittamisen.

”Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.” (Talus ja muut, 2017, s. 13). Tämän oletusarvoisen tietosuojan periaatteen noudattamisen lisäksi yrityksen on dokumentoitava tarkoitus, jota varten tietoja käsitellään (Talus ja muut, 2017). Tietosuoja-asetuksen 25 artiklan (2016/679) mukaan käyttötarkoitukseen sopivalla tavalla on määriteltävä: kerättyjen henkilötietojen määriä, käsittelyn laajuus, säilytysaika ja tietojen saatavilla olo.

4.4 Tietosuoja-asetuksen vaatimusten noudattamisen osoittaminen

Tikkinen-Piri ja muut (2017) ehdottavat tietosuoja-asetuksen vaatimusten noudattamisen osoittamisen keinoiksi käytännesääntöjen ja sertifiointejen hankkimisen. Vaikka edellä mainitut keinot ovat yrityksille vapaaehtoisia, ne ovat suositeltavia. Alakohtaisten käytännesääntöjen on oltava esimerksi valvontaviranomaisen

hyväksymiä. Tietosuoja-asetuksen (2016/679) 40 artikla huomauttaa, että käytännesääntöjen on huomioitava eri sektorien erityispiirteet ja erikokoiset yritykset.

4.5 Tietomurtojen ja tietoturvaloukkausten käsittely

Tietosuoja-asetuksessa (2016/679) määritellään yrityksille ohjeet tietoturvaloukkaukseen puuttumisesta. Tietoturvaloukkaukseen on reagoitava loukkauksen aiheuttaman tai mahdollisesti aiheuttaman vahingon suuruuden perusteella. Erityisesti on huomioitava tietoturvaloukkauksen rekisteröidyille aiheuttamat vahingot.

Tietoturvaloukkauksesta on uuden asetuksen mukaan ilmoitettava 72 tunnin kuluessa tapahtuneesta. Ilmoitusta ei tarvitse tehdä, jos tietojenkäsittelijä pystyy osoittamaan, ettei tietoturvaloukkauksesta aiheudu luonnollisen henkilön oikeuksiin tai vapauksiin kohdistuvaa riskiä. Tästä syystä henkilötietojen käsittelijän on ymmärrettävä tietoturvaloukkauksia, jotta he pystyvät arvioimaan niiden vakavuutta ja vaikutuksia. Tietosuoja-asetuksessa tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen, taikka pääsy tietoihin. (2016/679.)

Saarion ja Vesterisen tekemän kyselytutkimuksen mukaan yleisimpiä tietoturvaloukkauksia yrityksissä vuonna 2017 olivat:

- Tietoverkkoon murtautumisen tai hakkeroinnin yritys,
- Kriittisistä yritysasioista kertominen luvatta kolmannelle osapuolelle,
- Tietojen luvaton kopiointi ennen siirtymistä pois yrityksen palveluksesta,
- Yritystiedon (sisällön) luvaton urkkiminen / vakoilu,
- Identiteetti on kaapattu tai yritetty kaapata rikolliseen toimintaan,
- Tietoverkkoon murtautuminen tai hakkerointi,
- Luottamuksellista yritysasiaa sisältävän asiakirjan luovuttaminen luvatta kolmannelle osapuolelle,
- Tiedostojen tahallinen tuhoaminen.

Yrityksen työntekijöiden olisi hyvä tiedostaa nämä erilaiset tietoturvaloukkaukset. Tiedostamalla mahdolliset riskit, tietojenkäsittelijä voi paremmin reagoida niihin. Tietoturvaloukkausten lisäksi poikkeamat yrityksen toiminnassa on tärkeä huomioida. Poikkeama toiminnassa saattaa olla merkki tietoturvaloukkauksesta (VAHTI-raportti, 2016).

Valtiovarainministeriön VAHTI-raportissa (1/2016) kehotetaan yritystä luomaan dokumentaatiopohja tietoturvaloukkauksesta ilmoittamiseen asianosaisille. Suomen Yrittäjät (2018) sivulla todetaan, että henkilötietojen käsittelijän on heti ilmoitettava rekisterinpitäjälle ja valvontaviranomaiselle tietoturvaloukkauksesta. Suomen Yrittäjät (2018) -tietosuojaoppaan ja VAHTI-raportin mukaan ilmoituksen on sisällettävä tietoturvaloukkauksen: selkeä kuvaus tapahtuneesta, asianomaiset, seuraukset, toimenpiteet ja mahdollisten haittavaikutusten lieventäminen.

4.6 Sanktiot asetuksen laiminlyönnistä

Tietosuoja-asetuksen laiminlyönnistä voi pahimmassa tapauksessa seurata suuret sanktiot. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta, sen mukaan kumpi näistä on suurempi. Valvontaviranomaisella on oikeus määrätä muitakin seuraamuksia tapauskohtaisesti erilaisista rikkomuksista. (VAHTI-raportti, 2016.) Tietosuoja-asetuksen mukaan vähäisestä rikkomisesta riittää huomautus (2016/679).

Hallituksen esitys (9/2018) uudesta tietosuojalaista sisältää pykälän 9 tietosuojarikos: ”Pykälän 1 momentissa säädettäisiin, että henkilö, joka muutoin kuin yleisessä tietosuoja-asetuksessa tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin yleisessä tietosuoja-asetuksen, tietosuojalain, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain tai henkilötietojen käsittelyä koskevan muun lain henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, olisi tuomittava tietosuojarikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.” (HE 9/2018.)

4.7 Tietosuojavastaava

Tietosuoja-asetuksen (2016/679) mukaan tietosuojan noudattamisen hallinnointi on mahdollisesti valtuutettava yrityksessä tietosuojavastaavalle. Tietosuoja-asetuksen (2016/679) artiklan 37 mukaan yrityksen on nimettävä tietosuojavastaava, jos joku seuraavista ehdoista täyttyy:

- *Tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin;*

- *Rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa; tai*

- *Rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä.*

Tietosuojavaltuutetun tehtäviä ovat: tiedonanto tietosuojasäännösten velvollisuuksista tietojenkäsittelijöille, asetuksen noudattamisen seuraaminen, antaa tietoja tietosuojaa koskevasta vaikutustenarvioinnista ja yhteistyö valvontaviranomaisen kanssa (Tietosuoja-asetus, 2016/679).

4.8 Henkilötietojen käsittelijän velvollisuudet

Tässä tutkimuksessa tiedonanto rekisteröidylle tapahtuu tilitoimiston ja sen asiakkaan sopimuksessa määritellyllä tavalla. Taloushallintoliitto (2018) tarjoaa asiakkailleen nettisivullaan sopimuspohjan henkilötietojen käsittelystä, joka on tietosuoja-asetuksen vaatimusten mukainen. Sopimuspohja sisältää sopimuksen henkilötietojen käsittelystä, selosteen käsittelytoimista, henkilötietoturvan tilitoimistossa ja asiakkaan antaman ohjeistuksen henkilötietojen käsittelystä. Tilitoimisto toimii henkilötietojen käsittelijänä

ja käsittelee asiakasyritysten eli rekisterinpitäjien lukuun henkilötietoja tietojenkäsittelysopimuksen määrittämällä tavalla. Asiakasyritys määrittelee siis tietojenkäsittelyn ohjeistuksen tilitoimistolle, joka kirjataan toimeksiantosopimukseen.

Tietosuoja-asetuksen 28 artikla (2016/679) käskee henkilötietojen käsittelijän noudattamaan rekisterinpitäjän ohjeistuksia ja dokumentaatiota henkilötietojen käsittelystä. Tietosuoja-asetuksen (2016/679) 28 artikla määrittää sopimuksen sisältöä: ”Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet.”

Valtiovarainministeriön laatimassa raportissa suositellaan erilaisia toimenpiteitä tietosuoja-asetuksen noudattamiseen ja määritellään henkilötietojen käsittelijän velvollisuuksia:

- *Käsittelee henkilötietoja ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti eli huomioi henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit,*
- *Noudattaa salassapitovelvollisuutta,*
- *Toteuttaa tietoturvallisuuden henkilötietojen käsittelyssä tietosuoja-asetuksen vaatimilla toimenpiteillä,*
- *Ei ulkoista henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta,*
- *Auttaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa,*
- *Auttaa rekisterinpitäjää käsittelyn tietoturvallisuuden toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa, vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa tietosuoja-asetuksen mukaisesti,*
- *Joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle käsittelypalvelujen päättyessä, sekä poistaa niistä hallussaan olevat kopiot ja*
- *Sallii rekisterinpitäjän suorittaa auditoinnit ja osallistuu niihin itse. Käsittelijän tulee myös saattaa rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen asetuksen velvollisuuksien noudattamisen osoittamista varten.*

(VAHTI-raportti, 2016.)

4.9 Rekisteröidyn/Rekisterinpitäjän oikeudet ja velvollisuudet

Tietosuoja-asetukseen (2016/679) on koottu paljon tietoja koskien rekisteröityjen oikeuksia, jotka henkilötietojen käsittelijän on huomioitava. Taloushallintoliiton mukaan henkilötietojen käsittelijän on sovittava rekisteröityjen oikeuksien toteuttamisesta yhteistyössä rekisterinpitäjän kanssa (Taloushallintoliitto, 2018).

Tietosuoja-asetuksen (2016/679) rekisteröidyn oikeudet:

- Oikeus saada käsittelyä ja keräämistä koskevat tiedot helposti ymmärrettävässä muodossa,
- Oikeus saada vastaus pyyntöihin ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa sekä oikeus saada perustelu kieltäytymiselle siinä tapauksessa, että rekisterinpitäjä ei aio noudattaa tällaista pyyntöä,
- Oikeus saada pääsy tietoihin,
- Oikeus tietojen oikaisemiseen,
- Oikeus tietojen poistamiseen,
- Oikeus käsittelyn rajoittamiseen,
- Oikeus siihen, että rekisterinpitäjä ilmoittaa henkilötietojen oikaisusta, poistosta tai käsittelyn rajoituksesta jokaiselle vastaanottajalle, jolle se on luovuttanut rekisteröidyn henkilötietoja,
- Oikeus siirtää tiedot järjestelmästä toiseen,
- Vastustamisoikeus,
- Oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn,
- Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta,
- Oikeus tehdä valitus valvontaviranomaiselle,
- Oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan ja
- Oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta.

Tietosuoja-asetuksen (2016/679) mukaan rekisteröidyllä on oikeus saada häntä koskevaa tietoa helposti ymmärrettävässä muodossa. Tietosuoja-asetuksessa useasti esiintyvä termi läpinäkyvyys tarkoittaa helposti ymmärrettävää ja saatavaa tietoa. Tietosuoja-asetus (2016/679) suosittelee mekanismien luontia, joilla rekisteröity voisi helpommin toteuttaa oikeutensa. Tällä tarkoitetaan sitä, että rekisteröity pystyisi helposti ja vaivattomasti näkemään hänestä kerätyt tiedot. Tietosuoja-asetuksen (2016/679) mukaan rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.

Tietosuoja-asetuksen (2016/679) ”oikeus tulla unohdetuksi” tarkoittaa henkilötietojen poistamista asiakkaan pyynnöstä. Tietosuoja-asetuksen (2016/679) 17 artikla kuvaa tarkemmin ”oikeutta tulla unohdetuksi” ja sen mukaan täytyy huomioida lakisääteinen esto artiklan noudattamiseen. Lakisääteiset säilytysajat kirjanpidon ja palkanlaskennan osalta kumoavat artiklan 17. Asiakkaan oikeuteen poistaa häntä koskevat tiedot, on huomioitava jatkossa edellä mainitut säilytysajat ja poistamisen tekninen toteutus. (VAHTI-raportti, 2016.) Asiakkaan oikeus tietojen siirtämiseen ja käsittelyn vastustamiseen on myös määritelty tietosuoja-asetuksessa (2016/679). Yrityksen on suunniteltava käytännöt myös näiden oikeuksien huomioimiseen.

Tietosuoja-asetuksen 21 artiklan vastustamisoikeus ei päde, kun; "..rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet tai jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi." (Tietosuoja-asetus 2016/679). Kirjanpitoon on lakisääteiset perusteet, joten sitä voidaan pitää perusteltuna syynä. VAHTI-raportin (2016) mukaan vastustamisoikeus ei päde, kun henkilötietojen käsittely on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten tai perustuu rekisteröidyn nimenomaiseen suostumukseen. Rekisteröidyn oikeudet riippuvat siis käsittelyn laillisuusperusteesta.

4.10 Dokumentaation ylläpito

Tietosuoja-asetuksen viidennen artiklan (2016/679) osoitusvelvollisuus on mahdollista toteuttaa luomalla yritykselle dokumentaatio tietosuojan noudattamisesta. Dokumentaatiosta ei ole tarkkoja vaatimuksia vaan se on suunniteltava yrityksen kokoon ja resursseihin nähden sopivalla tavalla. Tietotilinpäätös on hyvä vaihtoehto dokumentaatiosta ja osoitusvelvollisuuden näyttämisestä. (VAHTI, 2016.) Erilaisilla sertifikaateilla ja standardeilla yritys voi myös osoittaa noudattavansa tietosuoja-asetusta. Tehokas tietoturvallisuuden hallintajärjestelmä auttaa riskinhallinnassa. ISO 27000, ISO 27001 ja ISO 27002 standardit auttavat tehokkaan tietoturvallisuuden hallintajärjestelmän luonnissa. (Disterer, 2013.)

Tietosuoja-asetuksen (2016/679) 35 artikla vaatii yritystä suorittamaan tietosuojaa koskevan vaikutustenarvioinnin eli DPIA:n (data protection impact assesment), mikäli tietyntyyppinen käsittely aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Tikkinen-Piri ja muut (2017) määrittelevät tietosuojaa koskevan vaikutusten arvioinnin minimivaatimukset:

- Yleinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista,
- Arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta suhteessa tavoitteisiin,
- Arvio rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä ja
- Toimenpiteet riskien ratkaisemiseksi (eli suojatoimenpiteet, turvatoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan GDPR:n noudattaminen).

Miten valmistautua EU:n tietosuoja-asetukseen? -oppaassa määritellään tietosuojaa koskevan vaikutusten arvioinnin tarve:

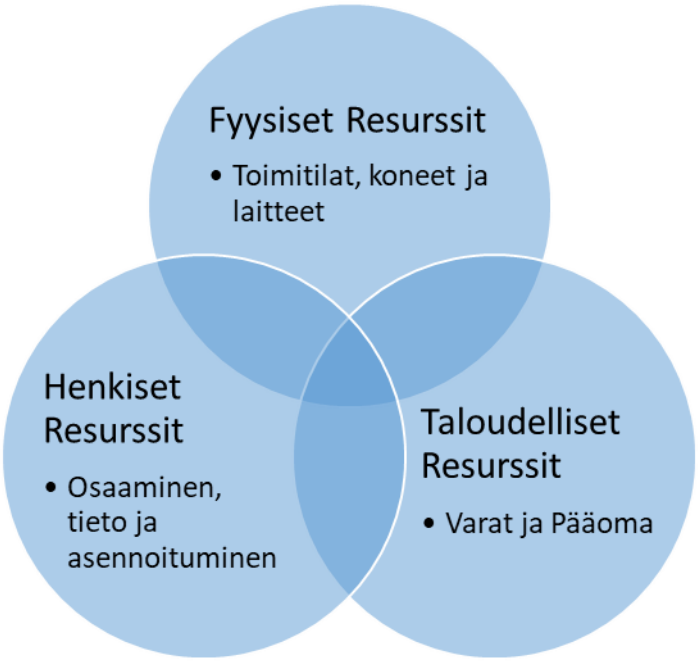
> "Vaikutustenarviointi on tehtävä erityisesti silloin, kun otetaan käyttöön uutta teknologiaa taikka, kun käsitellään laajamittaisesti rikostuomioita tai rikkomuksia taikka erityisiin henkilötietoryhmiin kuuluvia tietoja. Vaikutustenarviointi on tehtävä myös tilanteissa, joissa on kyse järjestelmällisestä ja kattavasta automatisoituun päätöksentekoon perustuvasta arvioinnista sekä tilanteissa, joissa on kyse yleisölle avoimen alueen järjestelmällisestä ja laajamittaisesta valvonnasta." (Talus ja muut, 2017.)

5. EU:n säännösten noudattaminen

Tässä luvussa käsitellään tutkimuksen toinen viitekehys eli tietosuoja-asetuksen noudattamisen luomat muutokset. Tikkinen-Piri ja muut (2017) toteavat, että tietosuoja-asetus aiheuttaa muutoksia yritysten toimintaan ja käytäntöihin. Yritysten on myös luotava dokumentaatiota käytännöistään ja toimintatavoistaan.

5.1 Muutoksenhallinta

Muutoksen suunnittelu on tärkeää, jotta muutoksen hallinta onnistuu hyvin. Muutossuunnitelman kannattaa sisältää muutoksen tavoitteet, keskeiset toimenpiteet, tekijät, muutostuen tarpeet ja aikataulu. Muutoksen hallintaan vaikuttavia keinoja ovat: avoin keskustelu, tuki, tiedotus, osallistuminen, jatkuva muutosviestintä, koulutus ja jatkon hallinta. (Luomala, 2008.) Luomala (2008) esittelee muutoksen suunnitteluun varattavat resurssit: fyysiset olosuhteet, taloudelliset varat, aika, tieto ja osaaminen, ja lisätyövoima. Muutokseen varattavia resursseja ovat siis kaikki yrityksen resurssit: fyysiset-, taloudelliset- ja henkiset resurssit (Alhola, 2016, s. 111-117).



Kuva 4. Yrityksen resursseja (Alhola, 2016, s. 111-117.)

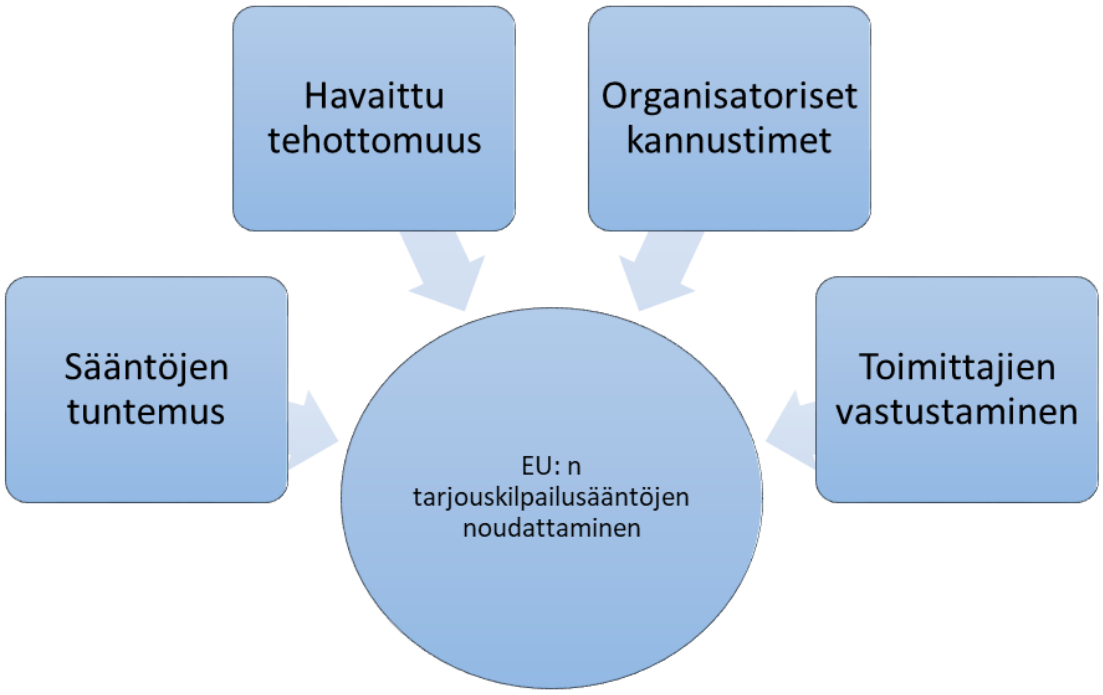
Yrityksen resursseilla tarkoitetaan henkilöstöä, toimitiloja, teknologiaa, koneita ja laitteita (Alhola, 2016, s. 46). Kuva 4 kuvaa yrityksen resursseja ja kuinka ne on jaettu kolmeen kategoriaan: fyysiset resurssit, henkiset resurssit ja taloudelliset resurssit. Näiden resurssien lisäksi yksi yrityksen tärkeistä resursseista on aika. Resurssien ylläpito ja suunnittelu ovat tärkeitä kilpailuetuja yritykselle. Resurssien suunnittelussa täytyy analysoida resurssien käyttöä ja tunnistaa negatiiviesti tai tehottomasti toimivat resurssit. (Alhola, 2016, s. 111-117.)

5.2 Malli EU:n direktiivien noudattamiseen

Tietosuoja-asetuksen noudattamista toimeksiantajayrityksessä tarkastellaan ja jäsennellään Geldermanin ja muiden (2006) luoman käsitteellisen mallin avulla. Tietosuoja-asetuksen luomat muutokset toimeksiantajayrityksessä havainnoitiin työntekijöiden haastatteluilla. Malliin on koottu neljä oletusta EU:n tarjouskilpailusääntöjen noudattamiseen. Tämä viitekehys valittiin tähän tutkimukseen, sillä perusteella, että sen avulla tunnistettiin EU:n tarjouskilpailudirektiivin noudattamiseen vaikuttavia tekijöitä. Myös tämän tutkimuksen tavoitteena oli selvittää EU:n säännösten noudattamiseen vaikuttavia tekijöitä, sekä jäsennellä niiden taustalla olevia syitä. Tietosuoja-asetus (2016/679) on myös EU:n säännös, jolla korvattiin aiemmin voimassa ollut direktiivi 95/46/EY, joten viitekehyksen noudattamisen tekijöitä voidaan perustellusti verrata siihen.

Geldermanin ja muiden (2006) tutkimuksessa aineisto hankittiin kyselyillä Alankomaiden puolustusministeriön ostoalan ammattilaisille, joita kyselyyn hyväksyttiin 147. Ammattilaiset oli valittu niin, että direktiivi selkeästi koski heidän toimintaansa. Gelderman ja muut (2006) toteavat, että sääntöjen noudattaminen voisi edistää muutosta julkisissa virastoissa ja vaikuttaa erilaisiin käyttäytymisiin ja näkemyksiin EU:n tarjouskilpailua koskevista direktiiveistä. Mwelu, Davis, Ke ja Watundu (2018) käyttivät Geldermanin ja muiden (2006) tutkimusta hyväksi julkisten tienrakennushankkeiden täytäntöönpanoa koskevan sääntelykehyksen noudattamisessa. Othman ja Suleiman (2013) analysoivat syitä huonoon asenteeseen työnteossa. Haastattelujen ja kyselyiden vastauksia verrattiin Geldermanin ja muiden (2006) tutkimukseen työntekijöiden motivoinnin osalta.

Gelderman ja muut (2006) esittävät käsitteellisen mallin EU:n tarjouskilpailudirektiivien noudattamisesta ja noudattamatta jättämisestä julkisissa hankinnoissa.



Kuva 5. Malli EU:n tarjouskilpailusääntöjen noudattamisen tekijöistä (Gelderman ja muut, 2006).

Kuvassa 5 on EU:n tarjouskilpailusääntöjen noudattamiseen mahdollisesti vaikuttavat tekijät. Sääntöjen tuntemuksella tarkoitetaan sitä, että direktiivin noudattajat eivät ole täysin selvillä direktiivin luomista säännöistä. EU:n direktiivit luovat uusia toimintatapoja ja ohjeita, joita EU-maiden on noudatettava. Sääntöjen noudattaminen voi olla haastavaa, jos yrityksen työntekijät eivät ymmärrä direktiivin luomia vaatimuksia ja kuinka noudattaa niitä työssään. Havaitulla tehottomuudella tarkoitetaan sitä, että direktiivit aiheuttavat tehottomuutta tiukoilla säännöksillä. Tehottomuudella tarkoitetaan sitä, että työntekoon varatut resurssit eivät riitä työtehtävien suorittamiseen. Resursseja ovat esimerkiksi aika ja henkilöstön määrä. (Syvänen, 2003.) Direktiivien luoma hallinnollinen taakka ja paperitöiden kuluttama aika voi myös aiheuttaa tehottomuutta (De Boer & Telgen, 1998). Tämän perusteella ylimääräinen työ voi aiheuttaa havaittua tehottomuutta direktiivien noudattamiseen. Organisatoriset kannustimet tarkoittavat, että johto luo kannustimia, joilla työntekijät saadaan toimimaan kannattavalla tavalla. Myös asetetuilla sanktioilla on vastaava vaikutus, jos ohjeita ei noudateta yritys voi määrätä sanktioita noudattamattomuudesta. Toimittajien vastustamisella tarkoitetaan sitä, että toimittajilla on oikeus valittaa, jos ostaja ei noudata direktiiviä. Tästä syystä noudattaminen on kannattavaa, jotta toimittajat ovat halukkaita yhteistyöhön myös jatkossa. (Gelderman ja muut, 2006.)

6. Aikaisempia tutkimuksia

Tässä luvussa käsitellään aikaisempi tutkimus EU:n uuden tietosuoja-asetuksen eli GDPR:n (General Data Protection Regulation) noudattamisesta. Noudattamisella tarkoitetaan asetuksen luomien ohjeiden ja käytäntöjen ottamista osaksi yrityksen ja sen työntekijöiden toimintaa. Toimeksiantajayritys toimii taloushallinnon alalla, joten tietosuoja-asetusta tarkastellaan taloushallinnon näkökulmasta (Financial Management). Aiempaa tutkimusta hankitaan ensisijaisesti tietosuoja-asetuksen noudattamisesta, koska toimeksiantajyrityksen tilaama selvitys sisälsi ohjeet tietosuoja-asetuksen noudattamiseen. Tietosuoja-asetuksen rikkomisesta tai noudattamatta jättämisestä voidaan pahimmillaan määrätä suuria sakkoja (2016/679), joten yritykset joutuvat varmistamaan kunnolla noudattavansa asetusta. Aikaisempi tutkimus on rajattu vuodesta 2016 eteenpäin, koska tietosuoja-asetus julkaistiin toukokuussa 2016. Tietosuoja-asetuksen vaatimuksia tarkennetaan ja selvitetään koko ajan.

Taulukko 1. Tietokantahaut aikaisemman kirjallisuuden analysoimiseen

Tietokanta	**Hakusanat**	**Artikkeleiden määrä**
ACM Digital Library	GDPR Financial Management	1
ACM Digital Library	GDPR	40
ACM Digital Library	GDPR Compliance	8
IEEE Xplore - IEEE/IEE Electronic Library	GDPR Financial Management	2
IEEE Xplore - IEEE/IEE Electronic Library	GDPR	109
IEEE Xplore - IEEE/IEE Electronic Library	GDPR Compliance	27
ABI/INFORM Collection (ProQuest)	GDPR Financial Management	6
ABI/INFORM Collection (ProQuest)	GDPR	31
ABI/INFORM Collection (ProQuest)	GDPR Compliance	15
EBSCOhost	GDPR Financial Management	2
EBSCOhost	GDPR	4
EBSCOhost	GDPR Compliance	3

Hakutulokset pyrittiin rajaamaan vain empiirisistä tutkimuksista kertoviin artikkeleihin. Hakutuloksia empiirisen tutkimuksen rajauksella löytyi hyvin vähän tai ei ollenkaan,

joten tässä luvussa esitellään myös muita tutkimuksia, kuten kirjallisuuskatsauksia. Aikaisempaa tutkimusta haettiin mahdollisimman monesta kokotekstitietokannasta, jotta saatiin kokonaiskuva aiemman tutkimuksen määrästä. Taulukossa 1 on esitelty tietokantahakujen löydösten määrät ja käytetyt hakusanat. Hakusanoilla ”GDPR Financial Management” löytyi vain 1-6 tieteellistä artikkelia per tietokanta. Hakusanalla ”GDPR” tieteellisiä artikkeleja löytyi paljon enemmän, yhdestä tietokannasta artikkeleita löytyi 4-109. Kappaleessa 6.1 on esitelty kaikki löydökset, jotka sisälsivät EU:n uuden tietosuoja-asetuksen ja taloushallinnon. Kappaleessa 6.2 on esitelty laajemmin tietosuoja-asetukseen liittyviä artikkeleita, jotka valikoitiin sillä perusteella että ne keskittyvät tietosuoja-asetukseen valmistautumiseen tai noudattamiseen, kuten tämä tutkimus.

6.1 Tutkimus tietosuoja-asetuksesta taloushallinnossa

Jackson (2018) toteaa artikkelissaan, että monet pienet yritykset ja keskisuuret yritykset ovat valmistautumattomia EU:n uuden tietosuoja-asetuksen voimaantuloon, eivätkä ole valmiita noudattamaan asetuksen vaatimuksia 25.5.2018. Jackson (2018) viittaa artikkelissaan Mathew Lewisin sanoihin siitä, että data tulee olemaan yritykselle enemmän velkaa kuin varaa. Tämä johtuu siitä, että tietosuoja-asetuksen voimaantulon jälkeen yrityksellä on oltava entistä selkeämpi syy tiedon säilyttämiseen. Tästä syystä rahoitusalan henkilötiedon säilytyksen määrä tulee vähenemään. Artikkelissa todetaan myös EU:n uuden tietosuoja-asetuksen noudattamisen kulut yritykselle. Pienellä yrityksellä on vähemmän resursseja tietosuoja-asetuksen noudattamiseen, joka myös osaltaan vaikeuttaa asetuksen vaatimusten noudattamista pienessä yrityksessä.

Sydekum (2018) tuo esille artikkelissaan taloushallinnon asiakkaiden vaatimukset tietojenkäsittelyä kohtaan. Asiakkaat odottavat, että heidän tietonsa on turvassa applikaatioissa, älypuhelimissa, tableteissa ja pilvipalveluissa. Yritysten on siis taattava asiakkailleen tietoturva, sekä samalla EU:n uuden tietosuoja-asetuksen vaatimukset. Tietosuoja-asetuksen noudattamisella ja siitä ilmoittamalla yritys voi myös luoda kilpailuetua muihin saman markkinan yrityksiin. Tietosuoja-asetuksen noudattaminen voidaan tuoda esille läpinäkyvällä tietojenkäsittelyllä eli asiakas on tietoinen yrityksen tietojenkäsittelystä ja tietojen siirtelyä koskevista toimenpiteistä.

Duncan ja Zhao (2018) kuvaavat ongelmia ja riskienhallintaa pilvipalveluissa EU:n uuden tietosuoja-asetuksen noudattamisessa. Taloushallinnossa on neljä mahdollista riskitekijää; luotto, maksuvalmius, markkinat ja operatiivinen toiminta. Riskien tunnistamisen lisäksi täytyy ymmärtää riskien todennäköisyys sekä vaikutukset. Artikkelissa on myös esitelty riskien minimoinnin ohjeita. Ohjeet on jaettu luottoriskin, maksuvalmiusriskin, markkinariskin, toiminnallisen riskin, pilvitoiminnan riskin tai tietosuoja-asetuksen noudattamisen riskin alle.

Yhteenvetona EU:n uutta tietosuoja-asetusta ja taloushallintoa koskevasta kirjallisuudesta voidaan todeta, ettei aihealueita ole juurikaan vielä tutkittu yhdessä. Julkaistut artikkelit ovat kirjallisuuskatsauksia tietosuoja-asetuksen vaatimuksista, mutta empiiristä tutkimusta aiheesta ei vielä löydy.

6.2 Aikaisempi tutkimus tietosuoja-asetuksesta ja sen vaatimuksista

Krystlik (2017), keskittyy artikkelissaan tietosuoja-asetukseen valmistautumiseen ja valmistautumisen tärkeyteen. Hän myös tiivistää yrityksiin kohdistuvat vaatimukset, jotka ovat: oikeus tulla unohdetuksi, selkeä asianomaisen suostumus käsitellä

henkilötietoja, oikeus tietojen siirtämiseen, rekisterinpitäjän nimittäminen, dokumentoitujen toimintatapojen mukaan tapahtuvan tietojenkäsittelyn varmistaminen, kirjalliset menettelytavat, takuu etteivät tietoja käsittele ulkopuoliset ilman asiakkaan ja henkilötietojen käsittelijän lupaa, henkilötietojen käsittelijän täydelliset ja yksiselitteiset tiedot kerätyistä henkilötiedoista ja henkilötietoihin sovelletuista prosesseista, yksityisyyden suojaa koskeva politiikka selitetään selkeällä ja yksiselitteisellä kielellä ja ilmoitus tapahtuneesta tietosuojaloukkauksesta 72 tunnin sisällä.

De Hert ja Papakonstantinou (2016), selvittävät artikkelissaan tietosuoja-asetuksen taustalla olevia haasteita. Tutkimus pohjautuu aiempaan kirjallisuuteen aiheesta, sekä päivittämään tekijöiden aiempaa artikkelia tietosuoja-asetuksen julkaisusta. Terrorismin ja maahanmuuton vuoksi henkilötietojen suojelu ja käsittely on kerännyt huomiota. Myös teknologian huima kehitys on osallisena tietosuoja-asetuksen tarpeellisuuteen. Kuten Tikkinen-Piri ja muut (2017), myös De Hert ja Papakonstantinou (2016), käsittelevät tietosuoja-asetuksen (2016/679) artikloja verrattuna vuoden 1995 henkilötietodirektiiviin 95/46/EY, jonka tietosuoja-asetus (2016/679) tulee korvaamaan. De Hert ja Papakonstantinou (2016), kirjoittamassa artikkelissa tuloksena on se, että tietosuoja-asetus antaa hyvät työkalut tulevaisuuden ongelmiin, mutta vastuu jää niiden käyttäjille. Työkalujen käyttäjien tueksi tulee myös artikkelin mukaan syntymään uudenlaisia toimialoja. Esimerkkejä näiden toimialojen toimijoista ovat tietosuojavaltuutetut, sertifiointielimet ja vaikutustenarviointien tekemistä tukevat palvelut. Tämän artikkelin ulkopuolelle jäävät kansainväliset tiedonsiirrot, akateemisten, tieteellisten, historiallisten ja siihen liittyvien tarkoitusten käsittely, aikaisemman ennakkokuulemisvaatimuksen ja tietosuojavaltuutetun rooli, joita suositellaan tulevaisuuden tutkimuskohteiksi.

Gellert (2018), perehtyi artikkelissaan tietosuoja-asetuksen artiklaan 35, joka käsittelee tietosuojaa koskevaa vaikutustenarviointia. Tutkimuksen tavoitteena on ymmärtää riskin käsite tietosuoja-asetuksessa. Tutkimusmenetelmänä on aiemman kirjallisuuden analysointi. Tietosuojaa koskeva vaikutustenarviointi on riskiperusteinen lähestymistapa tietosuoja-asetuksen noudattamiseen. Riskien kartoittaminen ja analysointi ovat tärkeässä asemassa tietosuoja-asetuksessa, varsinkin korkean riskin mahdolliset uhkat on tärkeä huomioida henkilötietojen käsittelyssä. Korkean riskin uhalla tarkoitetaan vaikutuksia kohdehenkilön oikeuksiin ja vapauksiin. Vaikka artikkelissa perehdytään tietosuoja-asetuksen tietosuojaa koskevaan vaikutustenarviointiin, riskin merkitys tietosuoja-asetuksessa todetaan lähes merkityksettömäksi tutkimuksen tuloksissa.

Zerlang (2017) käsittelee ja arvioi tietosuoja-asetuksen (2016/679) vaikutuksia tietoverkkoturvallisuuteen ja sen noudattamiseen aiemman kirjallisuuden avulla. Kuten De Hert ja Papakonstantinou (2016), myös Zerlang (2017) huomioi teknologian hurjan kehitysvauhdin. Tietosuoja-asetus tekee tietoturvallisuuden noudattamisesta ja käyttöönotosta välttämättömyyden, kun pelkkä turvallisuuden ymmärtäminen ei enää riitä toiminnallisen tehokkuuden saavuttamiseen. EU:n tietosuoja-asetuksen päätavoite on vahvistaa ja harmonisoida yksilön tietosuojaa. Taloudellisten sanktioiden avulla varmistetaan asetuksen noudattaminen ja asetuksen mukainen dokumentaatio tietosuoja-asetuksen vaatimuksista. Artikkelin tuloksena ja tulevaisuuden tutkimuskohteeksi määritellään yrityksen digitalisointistrategiat, jotka mahdollistavat yritysten siirtymisen digitaaliseen tulevaisuuteen. Digitaalisella tulevaisuudella tarkoitetaan tietosuoja-asetuksen noudattamista ja Big Datan hyödyntämistä liiketoiminta- ja turvallisuuspäätöksissä.

Sirur, Nurse ja Webb (2018) toteavat tutkimuksessaan, että syvällistä laadullista tutkimusta, jossa keskitytään organisaatioiden käsityksiin ja kokemuksiin tietosuoja-

asetuksen noudattamisesta, ei ole vielä tehty. Heidän tutkimusmenetelmänään ovat haastattelut, joissa kohdehenkilöiltä kysyttiin mielipiteitä ja ajatuksia tietosuoja-asetuksesta ja sen noudattamisesta. Tutkimuksen tavoitteena oli selvittää, mitä tietosuoja-asetuksen kanssa työskentelevät ajattelivat asetuksesta ja millainen prosessi tietosuoja-asetuksen käyttöönotto on heidän mielestään. Tutkimuksen havaittiin pk-yritysten eli pienten ja keskisuurten yritysten vaikeudet ja haasteet tietosuoja-asetuksen noudattamisessa. Pienemmillä yrityksillä on käytössään vähemmän resursseja, joita tietosuoja-asetuksen noudattaminen vaatii. Onnistunut käyttöönotto ja sen ymmärtäminen helpottaa uusien säännösten noudattamisessa.

Priyadharshini ja Shyamala (2018) käsittelevät kirjallisuuskatsauksessaan vaatimukset yritykselle noudattaa tietosuoja-asetusta. Tutkimusongelmana ovat tietosuoja-asetuksen noudattamisen haasteet. Tutkimuksen tuloksena ovat tiivistettynä tietosuoja-asetuksen vaatimukset yrityksille ja organisaatioille. Vaatimukset ovat yleisellä tasolla, eikä niitä ole kohdennettu määrätyn alan tai määrätyn kokoiselle yritykselle tai organisaatiolle.

Cvik, Pelikánová ja Malý (2018) tutkivat tietosuoja-asetuksen noudattamista. Tutkimuksen tavoitteena on tieteellisesti tunnistaa, ennustaa ja analysoida tietosuoja-asetuksen valikoituja ongelmakohtia ja sen käyttöönottoa erityisesti Tšekin kunnissa. Tutkimuksen tavoitteena on myös ehdottaa suosituksia siitä, miten minimoidaan tai jopa vältetään kielteiset vaikutukset. Tutkimusmenetelmänä tutkimuksessa on kirjallisuuskatsaus ja haastattelut. Tutkimuksen tuloksena huomattiin, että Tšekin kunnilla on vähäinen tietoisuus tietosuoja-asetuksen sisällöstä. Kunnat eivät myöskään ole valmistautuneet tietosuoja-asetukseen, koska eivät tiedä kuinka siihen pitäisi valmistautua. Tutkimuksen tuloksena ovat myös suositukset tietosuoja-asetuksen noudattamiseen:

1. EU:n pitäisi antaa hyvät helposti ymmärrettävät ohjeet ja tukea,

2. EU:n jäsenmaiden pitäisi tarjota resursseja ja auttaa tietosuoja-asetuksen kohteena olevia organisaatioita,

3. Yhdistysten ja muiden instituutioiden pitäisi yhdistää resurssejaan ja tarjota apua toisilleen,

4. Julkisen palvelun yksiköt hyötyisivät ulkoisista tietosuojavastaavan palveluista,

5. Jokaisen tietosuoja-asetuksen kohteena olevan pitäisi tarkastella tilannettaan, jotta tietosuoja-asetuksen noudattaminen onnistuu viiveettömästi.

Tietosuoja-asetuksen valmistautumista tai noudattamista koskevaa kirjallisuutta ei myöskään löytynyt kovinkaan paljoa. Empiiristä tutkimusta näistä artikkeleista löytyi vain kahdesta. Tietosuoja-asetuksen vaatimuksia on selkeästi aiemmassa kirjallisuudessa tutkittu paljon kirjallisuuden perusteella, mutta empiirinen tutkimus on harvinaisempaa. Tämän tutkimuksen tavoitteena on selvittää tietosuoja-asetuksen edellyttämät muutokset empriisenä eli käytännön tutkimuksena, jota ei aiemmasta kirjallisuudesta löytynyt varsinkaan taloushallinnon näkökulmasta.

7. Empiirisen tutkimuksen tausta ja tutkimusmenetelmä

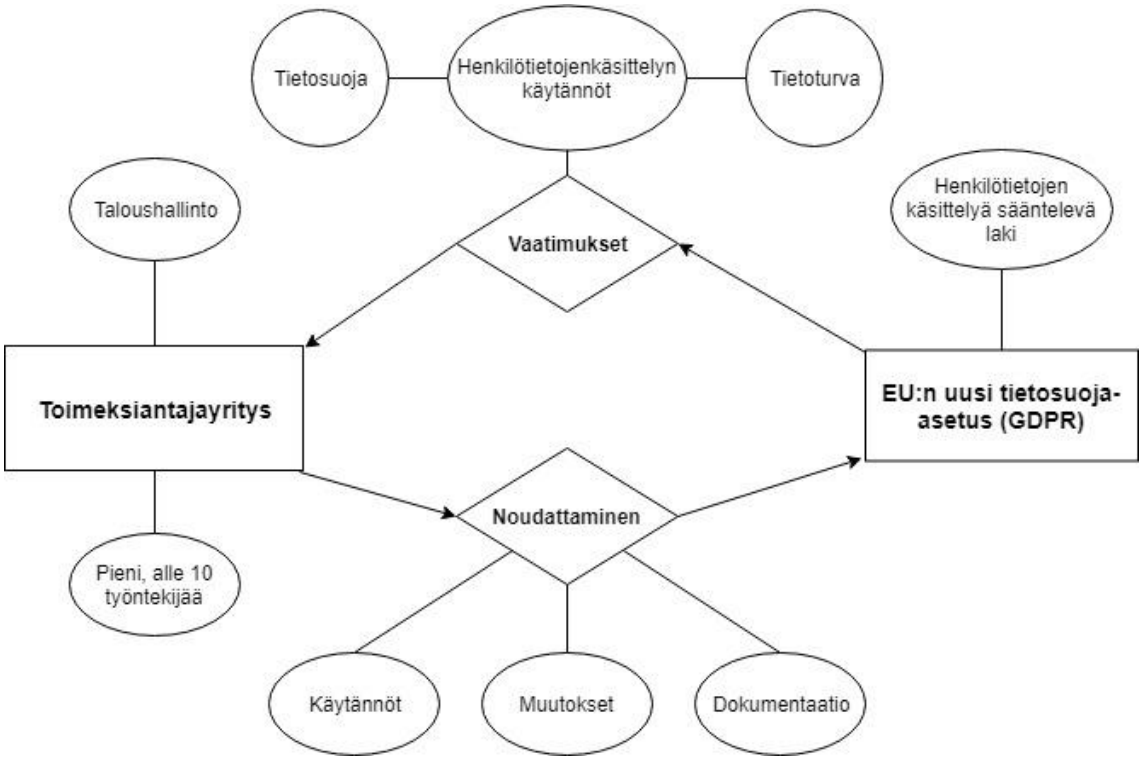
Tämä luku käsittelee empiirisen tutkimuksen taustoja. Luvussa esitellään tutkimuksen tavoitteet, tutkimusmenetelmät ja toimeksiantajayritys. Toimeksiantajayritys pysyy anonyymina, mutta luvussa esitellään tutkimuksen kannalta välttämättömät taustatiedot.

7.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena oli selvittää haastattelemalla yrityksen työntekijöitä, yrityksen nykytila EU:n uuden tietosuoja-asetuksen vaatimusten kannalta, sekä nykytilassa vaadittavat muutokset tietosuoja-asetuksen noudattamiseen. Nykytilalla tarkoitetaan tapoja ja käytäntöjä, joita työntekijät noudattavat työssään. Vaadittavat muutokset selvitetään vertaamalla yrityksen nykytilaa tietosuoja-asetuksen vaatimuksiin. Tietosuoja-asetus sisältää uusia vaatimuksia yrityksen tietojenkäsittelyyn ja luo siihen muutoksia. Haastatteluilla selvitettiin myös työntekijöiden oletuksia tietosuoja-asetuksen aiheuttamista muutoksista heidän omassa työssään ja yrityksen toiminnassa. Tutkimuskysymykset määriteltiin seuraavasti:

> Millainen yrityksen nykytila on tietosuoja-asetuksen vaatimuksiin nähden?
>
> Millaisia muutoksia EU:n uuden tietosuoja-asetuksen voimaantulo luo yrityksen toimintaan?

Toimeksiantajayrityksen tavoitteena oli saada selvitys/raportti nykytilastaan ja toimintaansa koskevista muutoksista ja toimenpiteistä, jotka EU:n uusi tietosuoja-asetus aiheuttaa, kun se tulee voimaan 25.5.2018. Raportti toimitettiin toimeksiantajayritykselle maaliskuussa 2018.



Kuva 6. Käsitteellinen malli tutkielman tavoitteesta

Kuvaan 6 on selvennetty tutkielman taustalla vaikuttavia tekijöitä, jotka muodostavat tutkielman tavoitteen ja vaikuttavat viitekehyksen valintaan. Kohteet on kuvattu suorakulmioihin, jotka ovat toimeksiantajayritys ja tietosuoja-asetus. Kohteiden suhteet on kuvattu timanttikuvioilla. Tietosuoja-asetus luo toimeksiantajayritykselle vaatimuksia, joita sen täytyy noudattaa. Kuvan nuolet kuvaavat suhteiden suunnan nuolen osoittamaan suuntaan. Kohteiden ja suhteiden ominaisuuksia on kuvattu palloihin.

Taulukko 2. Tutkimuksen viitehysten roolit

Viitekehys	**Rooli**
12 Tietosuoja-asetuksen vaikutuksen malli	Selvitetään toimeksiantajayrityksen työntekijöiden haastatteluja ja mallia vertaamalla puutteet tietosuoja-asetuksen noudattamisessa
EU:n tarjousdirektiivin noudattamisen malli	Hyödynnetään mallia tunnistamaan erilaisia tietosuoja-asetuksen luomia muutoksia
Kirjallisuuskatsaus	Selvitetään aiempi tutkimus aiheesta

Taulukkoon 2 on koottu tutkimuksen viitekehykset ja niiden roolit. Tutkielma koostuu kolmesta viitekehyksestä.

7.2 Laadullinen tapaustutkimus

Tutkimuksen tutkimusmenetelmänä on laadullinen tapaustutkimus. Laadullisessa tutkimuksessa tavoitteena on ymmärtää tutkittavaa ilmiötä tutkittavien näkökulmasta (Sarajärvi & Tuomi, 2017, s.131). Tässä tutkielmassa tietosuoja-asetusta tutkittiin toimeksiantajayrityksen työntekijöiden näkökulmasta. Tapaustutkimuksella tarkoitetaan tutkimusta, jonka tavoitteena on ratkaista valittu tapaus tutkimuskysymysten avulla. Tutkimuskysymyksien muodostamiseen vaikutti tutkimuksen tavoite eli ratkaisu, joka on tietosuoja-asetuksen vaatimusten selvittäminen toimeksiantajayritykselle. Tietosuoja-asetuksen noudattaminen tilitoimistossa on tutkielman tapaus. Tapaustutkimuksessa tiedonhankintatapana voidaan käyttää haastatteluja, kuten myös tässä tutkimuksessa käytettiin. (Eriksson & Koistinen, 2005.)

Tutkimusmateriaali voi olla kvalitatiivista tai kvantitatiivista. Tämän tutkimuksen aineisto on kvalitatiivista eli laadullista materiaalia, joka hankittiin puolistrukturoiduilla haastatteluilla. (Eskola & Suoranta, 1998, s. 22-64.) Tutkimusmenetelmänä käytettiin puolistrukturoitua teemahaastattelua, jonka tarkoituksena on aineiston hankinta haastateltavien oman tietämyksen ja kokemuksen perusteella. Puolistrukturoitu haastatteluraakenne valittiin, jotta haastateltavilta saatiin paremmin kuvauksia vastauksiin tilanteeseen sopivilla apukysymyksillä. Haastattelua pyrittiin ohjaamaan haastateltavien omiin kokemuksiin ja toimintatapoihin. Sarajärvi ja Tuomi (2017, s. 66) määrittelevät, että teemahaastattelujen teemat perustuvat yleensä tutkimuksen viitekehykseen. Haastattelujen pääteemana oli tietosuoja-asetus, joka on myös viitekehyksen aiheena. Tietoturvan, tietosuojan ja tietosuoja-asetuksen aiheuttamat muutokset ja riskit yrityksen toiminnassa liittyvät olennaisesti tietosuoja-asetukseen, joten haastattelukysymykset on jaoteltu niiden perusteella.

Puolistrukturoidun ryhmähaastattelun ja yksilöhaastatteluiden lähteinä käytettiin Tikkinen-Piri ja muut (2017) artikkelia tietosuoja-asetuksen vaatimista muutoksista henkilötietoja käsitteleville yrityksille, Talus ja muut (2017) ohjetta valmistua EU:n tietosuoja-asetukseen, Luomala (2008) artikkelia muutoksen johtamisesta ja Tietosuoja-asetusta (2016/679). Haastattelujen suunnittelussa pyrittiin huomioimaan haastateltavien omat kokemukset ja tietämys tietojenkäsittelystä ja tietosuojasta. Muutosjohtamisen näkökulma tuotiin haastatteluihin, koska tietosuoja-asetuksen oletetaan luovan muutoksia yrityksen työntekijöiden työskentelyyn. Harrell ja Bradley (2009) jakavat puolistrukturoidut haastattelukysymykset kolmeen kategoriaan: kuvailevat, rakenteelliset ja vertailevat. Kuvailevia kysymyksiä käytettiin tässä tutkielmassa selvittämään haastateltavien työntekijöiden omia käytäntöjä ja toimintatapoja tietosuojan ja tietosuoja-asetuksen noudattamiseen. Rakenteellisillä kysymyksillä selvitettiin esimerkiksi toimeksiantajayrityksen toiminnan kannalta oleellisia asioita, kuten kerättyä tietoa, tiedon säilytystapoja ja resursseja. Vertailevia kysymyksiä hyödynnettiin apukysymyksinä, kun haastateltavaa pyydettiin kuvailemaan enemmän jo vastattuun kysymykseen. Jotta haastattelutilanteet onnistuivat, haastatteluissa noudatettiin ennalla suunniteltua protokollaa. Ensiksi esiteltiin haastattelija ja sen jälkeen haastateltavalle tiivistettiin haastettelujen tarkoitus sekä mainittiin, että haastattelut käsitellään anonyyminä. Haastateltaville myös mainittiin, että haastattelut poistetaan tutkimuksen jälkeen ja niitä käytetään vain tutkimustarkoituksiin. Kysymykset kysyttiin teemojen mukaan aikataulutetusti, koska haastatteluun oli ilmoitettu kestoksi yksi tunti. Lopuksi kiitettiin vastauksista ja kerrottiin raportin julkaisusta, joka oli haastateltaville tutkielman tavoite. (Harrell & Bradley, 2009.) Muut haastattelumenetelmät ovat strukturoitu ja avoin haastattelu. Strukturoitu haastattelu ei soveltunut tähän tutkimukseen, koska tavoitteena oli haastateltavien vastauksien saaminen heidän omien sanojensa avulla kuvailtuna. Strukturoitu haastattelu sisältää

valmiit vastausvaihtoehdot haastattelukysymyksiin, jolloin haastateltavan on vaikeampi selittää omia mielipiteitään. Strukturoitu haastattelu sopii paremmin määrälliseen tutkimukseen. (Sarajärvi & Tuomi, 2017, s.62.) Avoin haastattelu ei myöskään sovi tutkimukseen, koska haastateltavilla ei ollut tarkkaa tietämystä haastattelun aiheesta, joten ei voitu edetä täysin haastateltavan ehdoilla.

Tutkimukseen osallistuivat kaikki haastatteluhetkellä yrityksessä työskennelleet työntekijät eli yhdeksän henkilöä. Haastattelut toteutettiin yhtenä ryhmähaastatteluna ja kaikkien yrityksen työntekijöiden kanssa sovittiin, myös omat yksilöhaastattelut. Kaikki työntekijät osallistuivat yksilöhaastatteluihin, sekä ryhmähaastatteluun. Haastattelemalla kaikkia yrityksen työntekijöitä saatiin mahdollisimman tarkka ja realistinen kuvaus yrityksen tietämyksestä ja osaamisesta tietosuoja-asetuksesta. Tutkimuksen haastattelut toteutettiin kahdessa osassa, ensin ryhmähaastattelu joulukuussa 2017 ja sitten yksilöhaastattelut tammikuussa 2018. Haastattelut oli tärkeä suorittaa ennen EU:n uuden tietosuoja-asetuksen voimaantuloa, jotta toimeksiantajayritys saa todellisen käsityksen työntekijöidensä osaamisesta tarpeeksi ajoissa ennen tietosuoja-asetuksen voimaantuloa toukokuussa 2018.

Ryhmähaastatteluun osallistuivat kaikki yrityksessä haastattelujen aikaan työskennelleet työntekijät, joten haastatteluprosentti oli 100 %. Puolistrukturoidun haastattelun mukaan kaikki kysymykset käytiin läpi ja haastattelua jatkettiin lisäkysymyksillä vastausten mukaan. Haastattelukysymykset on esitelty tutkielman lopussa liiteessä yksi. Ryhmähaastattelun tavoitteena oli saada alustava kokonaiskuva työntekijöiden tietämyksestä aiheesta. Ryhmähaastattelun perusteella luotiin kysymysrunko yksilöhaastatteluille. Ryhmähaastattelun tavoitteena oli myös luoda ensimmäinen käsitys yrityksen tilanteesta tietosuoja-asetuksen tietämyksen ja osaamisen perusteella. Ryhmähaastattelu järjestettiin yhteisessä taukotilassa, johon vain yrityksen työntekijöillä on pääsy. Ryhmähaastattelun tavoitteena oli myös luoda keskustelua työntekijöiden välillä monipuolisten vastausten saamiseksi. Ryhmähaastatteluun aikaa oli varattu kaksi tuntia, jotta kaikki halukkaat ehtivät vastata kysymyksiin.

Yksilöhaastatteluihin osallistuivat kaikki yrityksessä haastattelujen aikaan työskennelleet henkilöt, jotka olivat osallistuneet ryhmähaastatteluun, joten haastatteluprosentti oli myös 100 %, kuten ryhmähaastattelussa. Kuten ryhmähaastattelu, myös yksilöhaastattelu oli puolistrukturoitu teemahaastattelu. Kaikki kysymykset käytiin läpi ja haastattelua jatkettiin lisäkysymyksillä vastausten mukaan. Haastattelukysymykset on esitelty tutkielman lopussa liitteessä kaksi. Yksilöhaastatteluiden tavoitteena oli käydä läpi ryhmähaastattelussa käytyjä asioita yksityiskohtaisemmalla tasolla. Yksilöhaastattelut toteutettiin työntekijöiden työhuoneissa, joihin haastatteluhetkellä oli pääsy vain haastateltavalla työntekijällä ja haastattelijalla, jotta työntekijällä oli mahdollisuus kertoa luottamuksellisesti omia oletuksia ja kokemuksia aiheiden tiimoilta. Kaikille työntekijöille esitettiin samat kysymykset, mutta puolistrukturoidun haastattelun mukaan lisäkysymykset erosivat haastattelun edetessä. Lisäkysymyksillä pyrittiin pysymään kysymyksen aiheessa ja täsmentämään haastateltavan vastauksia. Yksilöhaastatteluihin aikaa oli varattu tunti jokaista haastateltavaa kohden. Haastatteluiden aihe oli kaikille selvillä ryhmähaastattelusta.

Haastattelujen jälkeen aineisto litteroitiin eli kirjoitettiin puhtaaksi. Tekstimuotoista aineistoa yksilöhaastatteluista syntyi 34 sivua ja ryhmähaastattelusta viisi sivua riviväliällä yksi ja fonttikoolla 11. Jotta haastateltavat pysyivät anonyymina, haastateltavien nimet poistettiin jo litterointivaiheessa. Myös yrityksen nimi on anonyymi tässä tutkielmassa. Kuten tietosuoja-asetus (2016/679) kuvaa anonyymeja

tietoja: ”..tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole tai ei ole enää mahdollista.” Haastateltavien yksilöimisellä ei tässä tutkimuksessa ole merkitystä, koska toimeksiantajayritys tilasi kokonaiskuvan yrityksensä tilanteesta, jolloin yksittäisen työntekijän vastauksella ei ole merkitystä tutkimustulosten kannalta. Haastattelut on numeroitu juoksevasti Taulukossa 3; Haastateltava 1, Haastateltava 2 … Haastateltava 9. Haastateltavien anonyymisyyden suojaamiseksi haastateltavia ei identifioida tuloksia havainnallistavissa lainauksissa. Litteroinnin jälkeen suoritettiin aineiston analyysi.

Aineiston analyysimuodoksi valittiin teemoittelu ja teorialähtöinen analyysi. Eskola ja Suoranta (1998, s. 128) toteavat, että teemoittelu on suositeltava analysointitapa käytännöllisen ongelman ratkaisussa. Tässä tutkimuksessa käytännön ongelmana on tietosuoja-asetuksen noudattaminen. Aineisto teemoiteltiin teemahaastattelussa käytettyjen teemojen mukaisesti. Teemat ovat: Tietovirrat, tietovarannot, tietosuoja, riskit, tietosuoja-asetus ja muutokset. Tässä tutkimuksessa kirjallisuuskatsaus muodosti tutkielman viitekehyksen, joka vaikutti teemojen valintaan. Teorialähtöisessä sisällönanalyysissa teoreettiset käsitteet ovat tiedettynä ennen aineiston hankintaa. Tämän määritelmän nojalla aineistosta luodaan näkemys olemassa olevan teorian nojalla. Tässä tutkimuksessa kirjallisuuskatsaus toimii teoriana ja aineistona toimivat toimeksiantajayrityksen työntekijöiden haastattelut. Kirjallisuuskatsauksen ja haastatteluiden perusteella voidaan luoda näkemys henkilöstön tietosuoja-asetuksen (2016/679) vaatimusten noudattamisesta ja tietämyksestä. Teorialähtöisessä sisällönanalyysissa keskitytään tutkittavana olevaan ilmiöön eli haastatteluiden tulosta analysoidaan etsimällä yhteneväisyyksiä teoriaan, jolloin teoria ohjaa sisällönanalyysiä. Tässä tutkimuksessa tietosuoja-asetus otettiin ohjaavaksi tekijäksi lähes heti tutkimuksen alussa, joten päättely tapahtui deduktiivisesti. (Sarajärvi & Tuomi, 2017, s. 80–84.) Deduktiivisella analyysillä kaikkien haastateltavien vastaukset samaan kysymykseen koottiin yhdeksi, jolloin vastuksia verrattiin keskenään ja etsittiin yhteneväisyyksiä ja eroja. Deduktiivisella päättelyllä myös vahvistetaan tutkijan oletuksia. (Harrel & Bradley, 2009.) Teorialähtöisen sisällönanalyysin vaiheina ovat alkuperäisten ilmaisujen pelkistäminen yläluokasta alaluokkaan. Tässä tutkimuksessa yläluokat muodostettiin haastattelujen teemojen avulla ja alaluokat viitekehyksessä määriteltyjen luokiteltujen avulla, kuten Tikkinen-Piri ja muut (2017) määrittelemän 12 tietosuoja-asetuksen vaatimuksen ja Geldermanin ja muiden (2006) luoman käsitteellisen mallin avulla. (Sarajärvi & Tuomi, 2017, s. 95-97.)

Muut sisällönanalyysimenetelmät ovat; aineistolähtöinen sisällönanalyysi ja teoriaohjaava sisällönanalyysi. Teorialähtöisen ja teoriaohjaavan erot ovat melko pieniä. Teorialähtöisen ja teoriaohjaavan ero on teorian ottamisessa tutkimukseen. Teorialähtöisessä teoria otetaan mukaan heti alussa, kun taas teoriaohjaavassa se voidaan ottaa tutkijan valitsemassa vaiheessa. Tässä tutkielmassa teoria eli aiemman kirjallisuuden määrittelemä viitekehys otettiin mukaan jo haastattelukysymysten määrittämisessä ennen aineiston hankintaa. Aineistolähtöinen sisällönanalyysitapa ei myöskään sopinut tähän tutkimukseen, koska tutkielman aihe oli toimeksiantajayrityksen määrittelemä tietosuoja-asetus (2016/679) ja siihen liittyvä kirjallisuus. Aineistolähtöisessä sisällönanalyysissä käytettävä teoria määritellään aineiston keruun perusteella ilman selkeitä ennakko-oletuksia. (Sarajärvi & Tuomi, 2017, s. 80–84.)

7.3 Toimeksiantajayritys

Tutkimuksen kohderyhmänä oli pieni, alle 10 työntekijän tilitoimisto. Yhtiömuotona on osakeyhtiö, joten he noudattavat osakeyhtiölle asetettuja vaatimuksia ja lakeja. Osakeyhtiö on kirjanpitovelvollinen ja velvollinen laatimaan ja sisällyttämään tilinpäätökseensä konsernitilinpäätöksen. (Kirjanpitolaki 1336/1997.)

Taulukko 3. Haastateltavien työntekijöiden taustatiedot.

Haastateltava	**Ammatti**	**Tietämys tietosuoja-asetuksesta**
Haastateltava 1	Kirjanpitäjä	- Tietosuojakoulutus - Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Haastateltava 2	Esimies, Toimitusjohtaja	- Tietosuojakoulutus - Itsenäinen tiedonhankinta
Haastateltava 3	Kirjanpitäjä	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Haastateltava 4	Kirjanpitäjä	- Tietosuojakoulutus - Itsenäinen tiedonhankinta - Markkinointi ja mainokset
Haastateltava 5	Kirjanpitäjä	- Keskustelu kollegoiden kanssa
Haastateltava 6	Kirjanpitäjä	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Haastateltava 7	Kirjanpitäjä	- Tietosuojakoulutus - Itsenäinen tiedonhankinta
Haastateltava 8	Toimistosihteeri/kirjanpitäjä	- Itsenäinen tiedonhankinta - Keskustelu kollegoiden kanssa
Haastateltava 9	Kirjanpitäjä	- Tietosuojakoulutus - Itsenäinen tiedonhankinta

Haastatteluissa kartoitettiin ensimmäisenä työntekijöiden ja yrityksen taustatietoja. Taulukossa 3 on kuvattu työntekijöiden taustoja sekä tietämys ja mahdolliset koulutukset tietosuoja-asetuksesta. Jotta yritys säilyy anonyymina, tähän tutkimukseen on tuotu mahdollisimman vähän yritystä ja työntekijöitä kuvaavia asioita. Haastatteluiden aikaan talvella 2017 ja keväällä 2018 yrityksessä työskenteli yhdeksän henkilöä, joista kaikki osallistuivat ryhmähaastatteluun sekä yksilöhaastatteluihin. Haastateltavien kokemus yrityksestä ja taloushallinnon alalta vaihtelee alle vuodesta yli kymmeneen vuoteen. Haastateltavien työtehtävät koostuvat tilitoimiston palveluista. Tilitoimiston palveluihin kuuluu palkkahallinto, kirjanpito, laskutuspalvelut, verokonsultointi, sähköiset taloushallinnon palvelut ja muut taloushallintoon liittyvät neuvonta- ja konsultointipalvelut. Asiakkaita on monipuolisesti, erikokoisia yrityksiä, yhdistyksiä, kommandiittiyhtiöitä, säätiöitä, kiinteistöyhtiöitä sekä yksityisiä ammatinharjoittajia erilaisilla toimialoilla. Erilaisia asiakkaiden toimialoja ja ammatteja ovat esimerkiksi hammaslääkäri, lääkäri, hautaustoimisto, taksi, ravintola-ala, kauneudenhoitoala, kaupanala, kiinteistö- ja vuokraustoiminta-ala, asiantuntijakonsultointeja, maanrakennus, parturit ja Non-profitit eli yhdistykset ja säätiöt. Tilitoimiston toimintaan kuuluu myös olennaisena osana viestintä muihin organisaatioihin esimerkiksi verohallinto, kela, tilintarkastajat, pankit, vakuutusyhtiöt ja

taloushallintoliitto. Asiakkaita yrityksellä on Suomessa, Luxemburgissa, Saksassa, Belgiassa ja Ruotsissa, mikä omalta osaltaan pidentää tiedonsiirtojen etäisyyksiä.

8. Tulokset

Tässä tutkimuksessa tavoitteena oli saada tietoa yrityksen työntekijöiden tietosuojaosaamisesta ja –tietämyksestä sekä selvittää minkälainen heidän tietämyksensä taso on tietosuoja-asetuksen vaatimuksiin nähden. Lisäksi selvitettiin, millaisia muutoksia tietosuoja-asetus luo yrityksen toimintaan.

Ensimmäiseksi käsitellään ryhmähaastatteluissa syntyneet vastaukset tiivistetysti. Ryhmähaastattelujen tavoitteena oli pohjustaa aihetta keräämällä pohjatietoa yksilöhaastatteluja varten. Ryhmähaastattelussa epäselvät asiat kysyttiin laajemmin yksilöhaastatteluissa ja täysin selkeät asiat jätettiin pois. Toiseksi käsitellään yksilöhaastatteluiden tulokset kyselypohjan sisältämien teemojen mukaisessa järjestyksessä, paitsi riskit on eriytetty omaksi teemakseen. Haastattelut järjestettiin joulukuun 2017 ja helmikuun 2018 välillä, joten tietosuoja-asetuksen voimaantuloon ja noudattamiseen oli haastatteluhetkellä vajaa puoli vuotta.

8.1 Ryhmähaastattelu

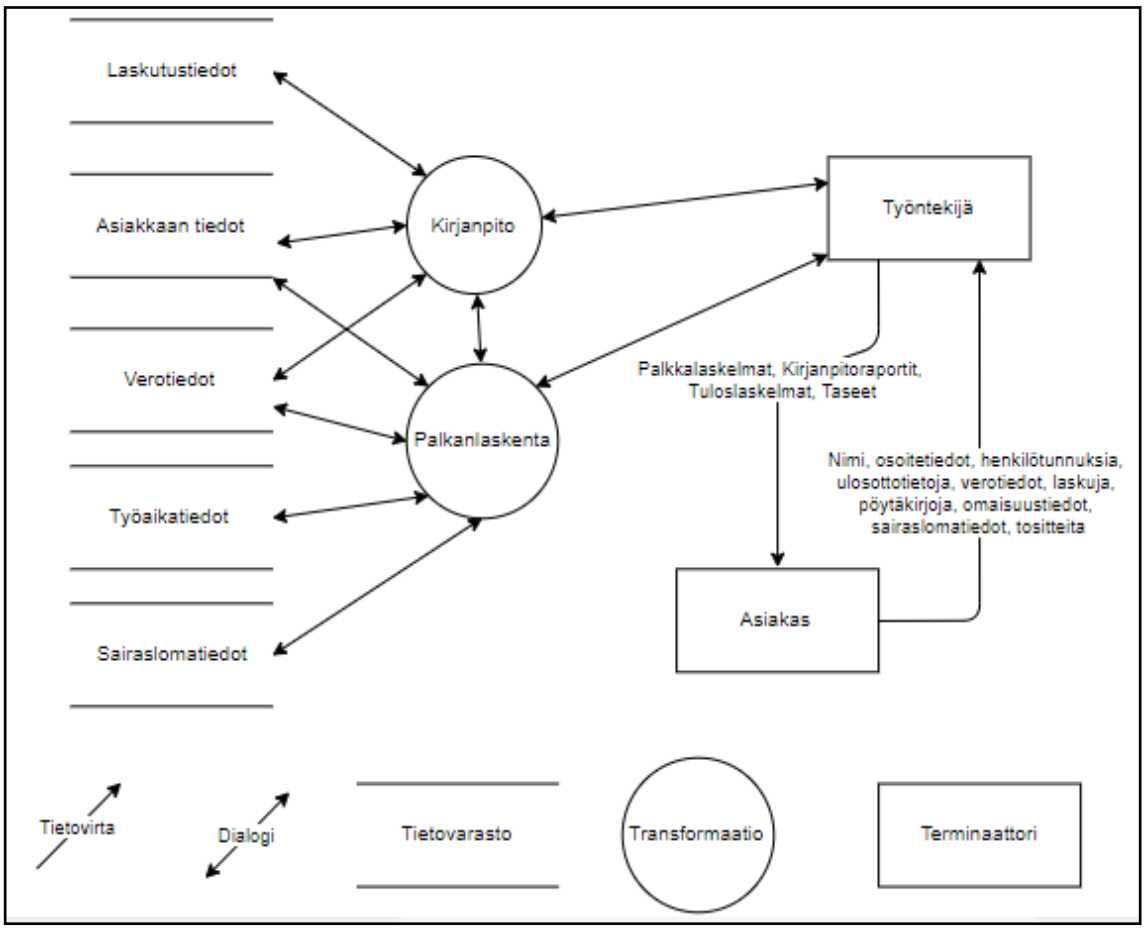
Ryhmähaastattelussa selvisi, että työntekijöillä ei ollut juurikaan tietämystä EU:n uudesta tietosuoja-asetuksesta. Käydyt vähäiset koulutukset koettiin erittäin suppeiksi, eikä niistä saatu irti mitään mainittavaa. Koulutukset olivat myös keskittyneet myymään tarkempia ohjeistuksia ja konsultointeja. Yhden haastateltavan mukaan palveluiden hinnat ovat melko kalliita pienelle tilitoimistolle. Tietosuoja-asetuksesta haastateltavat osasivat mainita isot sakot ja dokumentointivelvollisuuden. Haastateltavien mielestä arkaluontoista tietoa ovat: henkilötunnukset, terveystiedot, pankkitiedot, tilinumerot ja pankkitunnukset. Arkaluontoista tietoa ei käsitellä erillä tavalla muuhun henkilötietoon verrattuna. Haastatteluissa tietojenkäsittelyyn liitettiin useassa kohtaa sana ”luottamus”. Haastateltavien mielestä varsinkin Suomessa tilitoimistojen asiakkaat luottavat, että heidän tietojaan käsitellään sopivalla tavalla. ”Tilitoimistolla velvoite auttaa. Me kerrotaan miten pitää toimia ja minkälaisia dokumentteja on. Taloushallintoliitto myös luo ohjeistusta ja dokumenttipohjia.” (Ryhmähaastattelu). Yrityksessä tietojenkäsittelyä ei valvota millään tavalla sisältä tai ulkoa. Esille nostettiin luottamus ohjelmistotaloon, joka tarjoaa tilitoimiston pilvipalvelut kirjanpitoa ja arkistointia varten. Oletetaan, että ohjelmistotalo on sisällyttänyt palveluihinsa vaadittavan tietoturvan. Tietosuojavastaavaa yritys ei aio nimittää, koska nykyisen ohjeistuksen mukaan se ei ole pakollista. Ryhmähaastattelussa ilmeni, että yrityksessä ei ole nimettynä tietosuojavastaavaa. Tietosuojavastaava nimitetään vain pakon edessä. Yrityksen sisällä on tietosuoja-asetuksen noudattamisen valvominen nimitetty osalle henkilöstöstä, mutta kukaan heistä ei ole tietosuojavastaava. ”Se ohje, mikä tuli jostakin koulutuksesta, oli että, että, jos ei ole pakko nimittää, niin ei missään nimessä kannata nimittää. Koska siihen sisältyy niin valtava hallinnollinen taakka.” (Ryhmähaastattelu)

8.2 Yksilöhaastattelut

Tässä kappaleessa käsitellään yksilöhaastattelut koostettuna haastattelujen teemojen mukaisesti. Riskit on nostettu haastattelurungosta omaksi teemakseen, koska sillä on iso merkitys tietosuoja-asetuksessa.

8.2.1 Tietovirrat ja tietovarannot

Yrityksen tietovirrat ja tietovarannot selvitettiin, jotta saatiin kokonaiskuva yrityksen käsittelemästä tiedosta ja tietojenkäsittelytavoista.



Kuva 7. Tietovuokaavio yrityksen tietovirroista työntekijöiden haastattelujen perusteella

Yrityksen henkilötiedot, tietovarastot ja tiedonkäsittelykanavat on kuvattu kuvassa 7. Tietovuokaaviosta selviää tiedonkulku asiakkaalta tietojärjestelmiin.

Mitä tietovirrat mielestäsi ovat?

Neljä yhdeksästä työntekijästä vastasi tietovirtojen tarkoittavan tiedon kulkemista paikasta toiseen. Niillekin haastateltaville, jotka eivät varmaa tienneet, osasivat epäillä tiedon liikkumista paikasta toiseen. Haastateltavat myös totesivat, että tietovirta voi kulkea erilaisia reittejä, kuten sähköpostilla tai suullisesti. ”Kaikki se tietovirta mitä meille tulee sisälle ja lähtee ulos oli se sitten suusanallista tai sähköpostia tai muutoin kaikkien järjestelyn kautta virtausta.” (Haastateltava).

Mitä henkilötietoja käsittelet työssäsi?

Haastateltavien mukaan yrityksen käsittelemiä henkilötietoja ovat: nimet, henkilötunnukset, osoitetiedot, puhelinnumerot, sähköpostiosoitteet, verotiedot, palkkatiedot, sairaushistoria, lääkärillä käynnit, lääkärintodistukset, sairaslomat, vakuutusasiat, ammattiyhdistysjäsenmaksut, ulosotot, osingonsaajien tiedot, tulo- ja menotiedot, hallituksenjäsenten tiedot, tilinumerot, matkalaskut, työsopimusasiat, kauppakirjat, varainsiirtoasiat ja pankkitunnukset. Haastateltavien mielestä

arkaluontoista tietoa ovat: henkilötunnukset, terveystiedot, pankkitiedot, tilinumerot ja pankkitunnukset.

Mitä tietoa lähetät asiakkaille?

Haastateltavat lähettävät asiakkaille: asiakkaiden työntekijöiden tietoja, vuosi-ilmoituksia, kysymyksiä, vastauksia, tiliotteita, maksatuksentarkastuslistoja maksuista, virallisia asiakirjoja, raportteja, pöytäkirjoja, sopimuspapereita, palkkalaskelmia, kirjanpitoraportteja, veroilmoituksia, laskutustietoja, tilinpäätöstietoja ja laskuja.

Lähetätkö tietoa muille kuin asiakkaille?

Haastateltavat lähettävät tietoja asiakkaiden lisäksi; Vakuutusyhtiöihin, verohallintoon, projektien johtajille, pankeille, patentti- ja rekisterihallitulle (PRH), työkavereille, tilintarkastajille, ammattiliitoille, ammattiyhdistysliikkeille, ulosottovirastoon, kelalle, elinkeinoelämän keskusliittoon, kaupparekisteriin, työttömyysvakuutusrahastoon, urakoitsijoille ja isännöitsijöille.

Kuva 8. Toimeksiantajayrityksenä toimivan tilitoimiston sidosryhmiä

Kuvassa 8 on esitelty toimeksiantajayrityksen sidosryhmiä, joihin lähetetään erilaisia raportteja ja dokumentteja. Haastattelujen perusteella tilitoimiston sidosryhmiä ovat; vakuutusyhtiöt, ulosottovirasto, ammattiyhdistykset, urakoitsijat, pankit, kaupparekisteri, kela, verohallinto, asiakkaat ja ohjelmistotalo. Sidosryhmiä yrityksellä on paljon ja myös henkilötietoja joudutaan lähettämään niille ja takaisin. Sidosryhmien kanssa on sovittava muutoksista tiedonvälitykseen, jos tietosuoja-asetuksen voimaantulo niitä vaatii. Haastatteluissa ilmeni, että työntekijöiden mielestä rajapinnat näihin sidosryhmiin on oltava kunnossa, jotta tietosuoja-asetusta voidaan noudattaa. Kaikilla sidosryhmilläkin on velvollisuus noudattaa tietosuoja-asetusta, joten rajapinnat on hoidettava kuntoon yhteistyöllä.

Mitä tietoja saat asiakkailta?

Haastateltavat saavat asiakkailta nimiä, henkilötunnuksia, verotietoja, ulosottotietoja, ammattiyhdistystietoja, sairaslomatietoja, verotuspäätökset, yhtiöiden verotuspäätökset,

kuolinpesän veroilmoituspäätökset, tiliotteita, maksatuksentarkastuslistoja maksuista, virallisia asiakirjoja, exceleitä, sopimuspapereita, tietoja pankkitilien avaamisesta tai lainojen ottamisesta, pöytäkirja allekirjoitettuna, laskutukseen liittyviä tietoja, palkkalaskelmia, kirjanpitoraportteja, veroilmoituksia, omaisuustietoja, laskutustietoja, pankkitilitietoja, pankkitiliotteita, verotustietoja, kirjanpitoon tarvittavia kuitteja ja tositteita ja tuntitietoja. Haastateltavat myös totesivat, että työntekoon liittyvien tietojen lisäksi asiakkaat lähettelevät kysymyksiä, jolloin haastateltavalle voi päätyä tietoja, joita hän ei tarvitse. ”..asiakkaat haluaa paljon pohtia näitä palkanlaskijan kanssa, että mikä olisi hyvä tapa toimia.” (Haastateltava).

Millä tavoin tietoja lähetetään tai saadaan?

Yksilöhaastatteluissa haastateltavat pohtivat erilaisia tapoja tietojen lähettämiseen ja saamiseen. Haastateltavat lähettävät ja saavat tietoja; Sähköpostilla, postilla, sähköisten järjestelmien kautta, puhelimessa, post-it lapuilla, henkilökohtaisesti tuomalla ja tekstiviestillä. Haastattelujen mukaan sähköisten järjestelmien käyttöönotto riippuu asiakkaasta ja vaatii asiakkaan ohjausta järjestelmän käyttöönotosta. Asiakkaan on tarjottava tunnukset, jotta työntekijä voi ottaa järjestelmän käyttöön.

Mitä tietovarannot mielestäsi ovat?

Kukaan haastateltavista ei tiennyt mitä tietovaranto tarkoittaa. Useammalla haastateltavalla oli kuitenkin vahva arvaus tai epäily termistä; ”Sähköinen tai fyysinen paikka, mihin on säilötty tietoa. Varmaan vielä semmonen mistä sitä saa ehkä, pystyy niinku käyttämään.” (Haastateltava.) Seitsemän haastateltavaa epäili termin tarkoittavan tiedon säilyttämistä ja saatavuutta. Vain kaksi työntekijää ei tiennyt eikä osannut arvailla, mitä termi tarkoittaa.

Mitä tietovarantoja sinulla on käytössä, esimerkiksi henkilörekisterejä?

Haastattelujen perusteella työntekijöiden oli haastavaa ymmärtää tietovaranto tai heillä ei ollut tietämystä termistä. Haastattelujen perusteella yrityksen tietovarantoja ovat; yritysasiakkaiden henkilörekisterit, pilvi, sähköpostirekisteri, puhelinnumerot työpuhelimessa ja mapit.

Miksi keräätte ja säilytätte henkilötietoja, eli miten perustelet tietojen säilytyksen ja keräämisen?

Haastateltavat keräävät henkilötietoja lakisääteisesti ja ammatillisista syistä. Yrityksen sidosryhmät vaativat henkilötietoja osaan eteenpäin lähetettävistä dokumenteista. Säilytysajat ovat lakisääteiset, joten dokumentteja ja asiakirjoja on säilytettävä määrätty aika, ennen kuin ne on luvallista tuhota. Palkkojen laskemiseen yrityksen työntekijät tarvitsevat henkilötunnusta; ”Esimerkiksi palkkahallinnossa työntekijöitten vuosi-ilmoituksia tai muuta vastaavia ei pysty antamaan ilman henkilötunnusta.” (Haastateltava).

Missä henkilötietoa säilytetään?

Haastateltavien mukaan henkilötietoja yrityksessä säilytetään; palkanlaskennan kansioissa, kirjanpitoaineiston seassa, erilaisissa mapeissa, arkistossa, serverillä, pilvessä ja sähköpostissa. Eräs haastateltava kertoi, että myös muistitikkuja käytetään, mutta vain silloin kun asiakas poistuu tai vaihtaa tilitoimistoa. Myös tilintarkastajille tarkastettava aineisto annetaan muistitikulla. Monet haastateltavista myös totesivat, että sama tieto voi löytyä monesta paikasta.

8.2.2 Tietosuoja

Seuraavilla kysymyksillä selvitettiin työntekijöiden haastatteluilla yrityksen työntekijöiden tapoja tietojen suojaamiseen haastatteluhetkellä.

Millaisia vaikutuksia tietosuojalla ja sen noudattamisella on työhönne?

Haastatteluissa ilmeni, että monet haastateltavat työntekijät pohtivat tämän kysymyksen kohdalla tietosuoja-asetuksen luomia muutoksia. Osa yrityksen työntekijöistä oli perehtynyt tietosuoja-asetukseen koulutusten ja median kautta. Haastateltava oli käynyt useammassa tietosuoja-asetukseen liittyvässä koulutuksessa, joten hän ajatteli selkeästi jo tietosuoja-asetuksen vaatimuksia: *”Pitää paremmin huolta niistä mitkä mun vastuulla, pöydällä olevat paperit. Tuhottavat tuhottaviin. Miettiä, joka kerta onko tieto pakko säilyttää ja onko sen säilytykseen perusteet. Tosi paljon tehdään sitä, että säilytetään kaiken varalta. Varsinkin meijän ammattikunnassa on semmonen, että voidaan tarvia. Siitä poispääseminen tulee olemaan tosi hankalaa. Sitten tietenkin se, että myös asiakkainen tiedottaminen, siitä mikä on turvallinen tapa tietojen tietojenkäsittelyyn ja pyörittämiseen ja mitä ei.” (Haastateltava.)*

Työntekijät, jotka eivät olleet vielä tietoisia tietosuoja-asetuksen sisällöstä listasivat tietosuojan vaikutuksia;

- Ovet lukkoon,
- Paperit pois esiltä siivoojan tai asiakkaan käydessä,
- Silppuriin heti tuhottava tieto,
- Joitakin sähköposteja mahdollista aukaista vain kerran,
- Salasanat,
- Arkistointi ja
- Tietoja ei levitellä työpaikan ulkopuolelle.

Millaisia keinoja sinulla on tietovirtojen ja tietovarantojen suojaamiseen?

Työntekijät listasivat keinoja tietovirtojen ja tietovarantojen suojaamiseen;

- Lukot,
- Tietojen rajaaminen tiimeittäin,
- Käyttäjätunnukset ja salasanat,
- Salassapitovelvollisuus,
- Salasanojen päivittäminen,
- Omia tilanteenhallintatapoja ja
- Arkistointi.

Eräs haastateltava arvioi, että työntekijöihin voi luottaa, eikä heitä tarvitse valvoa.

8.2.3 Riskit tietojenkäsittelyssä

Riskejä selvitettiin yrityksen työntekijöiden näkökulmasta, jotta saatiin selville millaisia riskejä työntekijät tunnistavat työssään ja työympäristössään. Yrityksen työntekijät tunnistivat riskejä yrityksen toiminnassa. Riskien hallintaan ei otettu kantaa. Jokainen työntekijä käsittelee omalla tavallaan huomioimansa riskit.

Näetkö riskejä tietojen lähettämisessä tai saannissa (tietovirroissa)?

Työntekijöistä ainoastaan yksi uskoi tietojen lähettämisen ja saannin onnistuvan riskittömästi. Kaikki haastateltavat, jotka epäilivät lähettämisessä ja saannissa olevan riskejä, pohtivat sähköpostin riskejä. Vaikka kirjepostikin voi hukkua, sähköpostin riskit koetaan suuremmiksi. Asiakkaiden käyttämiin sähköisiin järjestelmiin ja niiden tietoturvaan luotetaan, koska järjestelmät tulevat isommilta toimijoilta, joten haastateltavien mukaan heillä pitäisi olla paremmat turvaukset. Toki tietojärjestelmissäkin tiedon lähetys on varmistettava. Voi sattua tilanne, jossa selvitys tai maksu ei tallennukaan järjestelmään. Sähköpostissa mahdollisia riskejä ovat; kaappaukset, hakkerointi ja vahingot. Vahingolla tarkoitetaan sitä, että haastateltava työntekijä saattaa laittaa viestin väärän osoitteeseen, jos ei ole tarkkana. Myös tunnistamisen kanssa täytyy olla tarkkana. Kun asiakas kysyy puhelimessa asioitaan, hänen henkilöllisyytensä täytyy olla varma ennen kuin tietoja uskaltaa luovuttaa.

Näetkö riskejä tietojen säilytyksessä (tietovarannoissa)?

Tietovarannoissa riskejä näki viisi haastateltavaa. Riskejä nähtiin pöydällä olevissa papereissa, hakkeroinnissa, etätyössä ja sähköpostissa. Siivoojaan käyminen huoneissa koettiin riskiksi, mutta myös todettiin, että; ”Siivoojalla vaitiolovelvollisuus” (Haastateltava.) Yhtenä riskinä nähtiin myös se, että kaikki työntekijät pääsevät kaikkeen arkistoituun tietoon käsiksi. Myös se, että arkistoissa säilytetään arkaluontoista tietoa, koettiin riskiksi. Salasanat säilytetään yrityksessä mapissa, jota kaikki pääsevät päivittämään. Yksi työntekijä otti salasanojen säilytyksen riskin esille, kun kysyttiin tietojen suojaamisen keinoja; ” Salasanatkaan ei ole vain minun tiedossa. […] Meillä on silleen, että kun minä vaihdan salasanan, niin käyn mappiin päivittämässä salasanan ja nään samalla kaikkien muidenkin.” (Haastateltava.)

8.2.4 Tietosuoja-asetuksen vaatimukset

Tietosuoja-asetukseen kohdistuvilla kysymyksillä selvitettiin yrityksen tietämystä tietosuoja-asetuksen vaatimuksiin nähden.

Onko sinulla hallussa henkilötietoja, joita et enää tarvitse tai sen säilyttämiseen syytä?

Kahdeksan haastateltavaa myönsi säilyttävänsä henkilötietoja, joita ei enää tarvitsisi. Heistä viisi totesi, että sähköpostissa voi hyvinkin pyöriä vanhoja viestejä, joiden säilyttämiseen ei ole syytä. Palkkahallinnon materiaalia on säilytetty ikuisesti, vaikka niitä täytyy säilyttää vain 10 vuotta, jonka jälkeen materiaali tuhotaan. Säilyttämistä perustellaan sillä, että tietoja voidaan vielä jossakin vaiheessa mahdollisesti tarvita. Tarpeettoman tiedon läpikäynti on myös aikaa vievää, eikä työntekijöillä ole ylimääräistä aikaa tietojen järjestelyä varten.

Kaikki kahdeksan haastateltavaa, jotka myönsivät säilyttävänsä ylimääräistä tietoa, tiesivät että tiedot pitäisi tuhota, jos sitä ei lain mukaan tarvitse säilyttää. ”Iso kynnys tuhota asiakkaan materiaalia, enkä oo lähteny lähettämään takaisin asiakkaille.” (Haastateltava.)

Missä maissa sinulla on asiakkaita?

Yrityksellä ei ole tällä hetkellä asiakkaita Euroopan ulkopuolella. Asiakkaita on Suomessa, Ruotsissa, Belgiassa, Saksassa ja Luxemburgissa.

Oletko tietoinen yrityksen tietosuojakäytännöistä?

Haastatteluissa selvisi, ettei kukaan yrityksen työntekijöistä ollut täysin varma yrityksen tietosuojakäytännöistä. Monet työntekijöistä totesivat, ettei tietosuojakäytäntöjä ole määritelty ollenkaan. Tällä hetkellä yrityksellä ei ole kirjallista dokumentaatiota tietosuojan noudattamisesta. Yksi haastatelluista totesi, että käytännöt ovat hyvät, ne pitäisi vielä dokumentoida. Ohjeistus on ollut suullista ja kaikilla ei ole siitä tietoa. Työntekijät arvioivat itse tietosuojan noudattamisen oman tietämyksensä perusteella. Työntekijöiden ja siivoojien kanssa tehdyt salassapitosopimukset kieltävät yrityksen sisäisen tiedon jakamista ulkopuolisille. Tietosuojaa noudatetaan tuhoamalla arkistoista tiedot, joiden lakisääteinen säilytysaika on päättynyt. Ovet pidetään lukossa, kun poistutaan huoneista. Kun asiakkaita käy toimistolla, paperit laittaan pois heidän näkyviltään. *”No tietenkin onhan meillä ollut puhetta, että pidetään paperit järjestyksessä, kasassa, mapeissa, kansioissa ja viedään arkistoon. Kuitenkin tässä on tosi monta vuotta pyöritetty papereita ja sähköiset järjestelmät olleet tässä verrattaen lyhyen aikaa. Enemmän paperipuolen tietosuojaan on panostettu kuin sähköisiin.”(Haastateltava.)*

Onko teidän alallanne alakohtaisia käytännesääntöjä tietosuoja-asetuksen noudattamiseen?

Neljä haastateltavista uskoivat, että käytännesääntöjä on olemassa, mutta niistä ei ole vielä ilmoitettu. Loput viisi eivät olleet tietoisia käytännesäännöistä. Erityisesti Taloushallintoliitolta odotetaan työntekijätason ohjeistusta.

Mikä on mielestäsi tietomurto tai tietoturvaloukkaus?

Yleisesti tietomurto ja tietoturvaloukkaus ymmärrettiin haastatteluissa hakkeroimisena, jolloin joku yrityksen ulkopuolinen henkilö ottaa haltuunsa tai katselee luvattomasti tietoja. Tällä hetkellä kukaan yrityksen työntekijöistä ei ollut varma oikeasta tavasta reagoida tietoturvaloukkaukseen. Jokainen reagoisi omalla tavallaan ja yrittäisi tehdä asialle jotain. Lähes kaikki kysyisivät apua joltain, esimerkiksi poliisilta, esimieheltä, ohjelmiston toimittajalta tai atk-osaajalta. Moni totesi haasteen tietoturvaloukkauksen huomioimisessa. Tietomurtoon tai tietoturvaloukkaukseen reagoimiseen ei ole yrityksessä ohjeistusta. Monet haastateltavat epäilivät, että oheistus puuttuu, koska vielä ei ole sattunut mitään. Vain yksi työntekijä totesi, että myös vahinko tai erhe voi olla loukkaus. ”Se on loukkaus jos me ollaan lähetetty toisen asiakkaan tietoja erheen vuoksi.” (Haastateltava.)

Tiedätkö mitä seuraa uuden tietosuoja-asetuksen laiminlyönnistä?

Yksilöhaastatteluiden perusteella kaikki yrityksen työntekijät tiesivät asetuksen laiminlyönnistä saatavat sakot. Monelle oli kuitenkin epäselvää, milloin sakot määrätään ja millä perusteella. Tällä hetkellä yrityksellä ei ole käytössä omia sanktioita,

vahingossa tapahtuneet tietosuojaloukkaukset hoidetaan keskustelemalla ja ratkaisemalla ongelma yhdessä. Ryhmähaastattelussa kaikki olivat yhtä mieltä siitä, että vahingossa tapahtuneesta rikkeestä selvitään keskustelemalla ja ongelman asianmukaisella hoitamisella. ”Pelottelu ja uhkailu on epäinhimillistä.” (Ryhmähaastattelu)

Kuinka reagoit asiakkaan pyyntöön saada häntä koskevat tiedot haltuunsa?

Asiakkaan pyyntö saada häntä koskevat tiedot haltuunsa on haastavaa toteuttaa, koska tällaista pyyntöä ei ole vielä kukaan asiakas esittänyt. Osa työntekijöistä kuitenkin huomioi tosiasian, että tiedothan ovat alun perin asiakkaan. ”Varmaan lähettäisin enkä kysyisi että miksi, koska hänen tietohan se alun perin on.” (Haastateltava.) Työntekijän täytyisi myös selvittää, missä kaikkialla tietoa oikeasti on, jos pyyntö koskisi kaikkia asiakkaan tietoja. Asiakkaan tunnistaminen pitäisi myös hoitaa tarkasti, jotta tiedot menevät varmasti oikealle henkilölle.

Ovatko asiakkaat antaneet suostumuksensa tietojensa käsittelyyn?

Asioiden hoitamiseen tarvitaan erilaisia tietoja asiakkaalta, joita ilman kirjanpitoa tai palkanlaskentaa ei voi suorittaa. Viisi haastateltavista totesi, että sopimukset asiakkaiden kanssa toimivat suostumuksena tietojenkäsittelyyn. Sopimukset täytyy uusia tietosuoja-asetuksen mukaisiksi. ”Taloushallintoliitto tarjoaa uudet sopimukset” (Haastateltava). Loput haastateltavista pohtivat, että kaikkea mitä asiakas toimittaa tilitoimistolle on lupa käsitellä ilman erillistä suostumusta.

Miten hoidat asiakkaan pyynnön poistaa häntä koskevat tiedot? ja miten hoidat asiakkaan pyynnön siirtää häntä koskevat tiedot?

Henkilötietojen käsittelijänä toimivalle tilitoimistolle ja sen työntekijöille voi tulla erilaisia tietopyyntöjä liittyen asiakasyrityksiin ja niiden työntekijöihin. Poistoja koskeviin asiakkaan tietopyyntöihin vaikuttaa monien asiakirjojen lakisääteiset säilytysajat, jotka on huomioitava. Asiakkaat toimittavat haastattelujen perusteella tilitoimistolle ja sen henkilökunnalle myös paljon erilaisia dokumentteja. Kaikille dokumenteille ja asiakirjoille ei ole tarkkoja tai välttämättä ollenkaan määrättyjä säilytysaikoja. Tietoa on myös säilötty useaan paikkaan. ”Vaatis ensin ajatusten kasaamista, että missä kaikkialla tietoa.” (Haastateltava) Työntekijöiden täytyisi pystyä kokoamaan eri paikoista tiedot ja määritellä niiden poistomahdollisuudet, jotta mahdolliseen pyyntöön voidaan reagoida. Pyyntöjä ei ole haastattelujen mukaan koskaan tullut, joten ohjeistusta niihin ei ole luotu. Yrityksellä on tietoja myös ulkopuolisen tarjoamassa pilvessä ja mapeissa. ”Siihen on käytäntö, että sähköisiä aineistoja ei poisteta, siihen pitäisi tehdä muutos.” (Haastateltava.)

Haastatteluissa ilmeni, että oikeus siirtää tiedot on taattu ohjeistuksella ja siirtoon on olemassa selkeä toimintakaava. Aikaisemmin on tapahtunut tilanne, jolloin on jouduttu todistamaan tietojen siirtäminen toiseen tilitoimistoon. Tästä syystä on laadittu ohje tietojen siirtämiseen. Tietojen siirtämisestä kerätään kirjalliset sopimukset asianosaisilta. Haastatteluissa kuitenkin ilmeni, että kaikki haastateltavat eivät olleet tietoisia ohjeesta ja toimintakaavasta. Kolme haastateltavista ei tiennyt tietojen siirtämisen ohjeesta.

Tiedätkö mitä tietosuojaa koskeva vaikutustenarviointi tarkoittaa?

Haastattelujen perusteella yrityksessä ei ole suoritettu tietosuojaa koskevaa vaikutustenarviointia. Yhdellekään yrityksen työntekijöistä ei myöskään ollut tietämystä termistä. Osa yritti arvailla termiä, mutta käyttivät sanoja ”Varmaan” ja ”Jotenkin”.

Tiedätkö mitä tarkoittaa rekisteriseloste tai tietosuojaseloste?

Haastattelujen perusteella yrityksessä ei ole tehty tietosuojaselostetta. Kaksi yhdeksästä työntekijästä tiesi, mitä termit tarkoittavat. Muilla joko ei ollut tietoa tai arvailivat. ”Rekisteriselosteessa on miten käytetään, missä säilytetään, kuka saa käyttää ja tietosuoja liittyy samaan.” (Haastateltava.)

8.2.5 Muutokset

Tässä kappaleessa käsitellään muutos-teeman alla kysytyt haastattelukysymykset, paitsi aiempi tietämys tietosuoja-asetuksesta, joka on koottu kappaleeseen taulukkoon kaksi. Näillä kysymyksillä selvitettiin yrityksen työntekijöiden mielipiteitä tietosuoja-asetuksen voimaantulosta ja ajasta sen jälkeen.

Millaisia vaikutuksia uudella tietosuoja-asetuksella ja sen luomilla muutoksilla on työhösi?

Työntekijät listasivat tietosuoja-asetuksen vaikutuksia omaan työhönsä;

- Tarkkuutta ja ohjeistusta tietojen käsittelyyn ja arkistointiin,
- Uudet tietojenkäsittelysopimukset, jotka sisältävät uudet ohjeet,
- Dokumentaatio,
- Henkilötietoja ei saa säilyttää varalta,
- Sähköpostin kanssa pitää olla tarkempi ja
- Turvallisuutta käytävä läpi.

Moni työntekijä totesi, ettei asetus luo juurikaan muutoksia ja muutokset riippuvat myös paljon asiakkaista ja ohjelmistojen toimittajasta. Osa asiakkaista ei halua mitään lisäkustannuksia, joten kalliita muutoksia ei haluta. Sähköpostin käyttöä pohdittiin paljon, kieltääkö vai salliiko asetus sähköpostin käytön tietojen lähettämisessä. Suuria muutoksia syntyy, jos sähköposti kielletään.

Millaisia vaikutuksia uudella tietosuoja-asetuksella on koko yrityksen toimintaan?

Työntekijät listasivat tietosuoja-asetuksen vaikutuksia koko yrityksen toimintaan;

- Turvallisuutta hyvä käydä läpi,
- Käytäntöjä tarkennetaan,
- Alkutyö asiakkaiden kanssa,
- Seurantaa,

- Kirjallinen dokumentaatio ja
- Rekisteriselosteet.

Osa haastateltavista työntekijöistä totesi, että ohjeita ja määrityksiä tulee ulkopuolelta, sidosryhmiltä ja asiakkailta. Koko prosessi tietosuoja-asetuksen noudattamisesta täytyy kaikkien työntekijöiden ymmärtää ja osata, joten se täytyy käydä läpi kunnolla.

”Miten niitä käsitellään, kuka pääsee käsittelemään, miten hävitetään? vaikutukset tulee ulkopuolelta. Rajapinnat täytyy olla kunnossa. […]. Totta kai meidänkin täytyy sopia, missä säilytetään, miten säilytetään, kuka pääsee, kuka ei pääse. […]Kun hyvin valmistelee ja hyvin tekee sen aloituksen, niin ei ole tarvetta palata asiaan.[…] Alkuvaiheessa rasittaa meitä, mutta me ei pystytä sitä laskuttaa mistään, joten menee omasta katteesta.” (Haastateltava.)

Mitä sinun mielestäsi yritys tarvitsee uuden tietosuoja-asetuksen noudattamiseen? esim. fyysiset olosuhteet, taloudelliset varat, aikaa, tietoa ja osaamista, lisätyövoimaa.

Työntekijät listasivat resursseja, joita tarvitaan tietosuoja-asetuksen noudattamiseen ja muutosten käyttöönottoon;

- Koulutusta,
- Sähköisiin järjestelmiin ominaisuuksia tietosuoja-asetuksen noudattamiseen,
- Aikaa,
- Tietoa,
- Osaamista,
- Ohjeistukset,
- Lisätietoa,
- Lisätyövoimaa,
- Alussa seurantaa uusien asioiden noudattamisessa,
- Uudet sopimukset asiakkaiden kanssa,
- Vastuiden jakamista,
- Perehtymistä ja
- Selvittää omaan työhön liittyvät vaikutukset.

Työntekijät myös pohtivat asiakkaina olevia pienyrittäjiä, joilla ei ole resursseja noudattaa tietosuoja-asetusta omin avuin. Monet asiakkaat varmasti kääntyvät tilitoimiston puoleen asetuksen noudattamisessa, joten työntekijät toivovat tietoa ja osaamista selittää asiakkaillensa tietosuoja-asetuksen vaatimukset myös heidän yrityksissään.

”Omat asiakkaat on tiukalla normaaliyrittämisessä, jos heillä pitää alkaa miettimään näitä juttua. Aikaa, rahaa ja hermoja palaa. Olisi hyvä jos pienelle yrittäjälle tulisi ohjeet. He muka määräävät meille tämän asian. Me tehdään paperit ja kerrotaan. Pitäisi olla tietoa. Meijän asiakkaille se olis todella haastavaa, jos ei konkreettisesti sanota, että tee näin.” (Haastateltava.)

9. Johtopäätökset ja pohdinta

Tämän tutkimuksen tavoitteena oli selvittää EU:n uuden tietosuoja-asetuksen vaatimuksia taloushallinnon alalla toimivan yrityksen työntekijöiden näkökulmasta. Työntekijöiden näkökulma selvitettiin yrityksen työntekijöiden haastatteluilla noin puoli vuotta ennen tietosuoja-asetuksen voimaantuloa. Haastatteluilla selvitettiin myös työntekijöiden olettamuksia ja käsityksiä tietosuoja-asetuksen voimaantulosta. Haastatteluihin osallistuivat kaikki yrityksen työntekijät, joten tutkimuksen tuloksia ja johtopäätöksiä voidaan pitää luotettavina koskemaan koko yrityksen toimintaa.

Tämän tutkielman ohella luotiin kohdeyritykselle raportti tietosuojan vaatimista muutoksista ja suositeltavista kehityskohteista, yrityksen tilaamana selvityksenä. Selvitys luotiin yhteistyössä yrityksen kanssa ja aineistonkeruumenetelmänä käytettiin haastattelua ja tutkimusmenetelmänä laadullista tapaustutkimusta. Raportti on lähetetty kokonaisuudessaan pelkästään tilitoimistolle, koska se sisältää heidän toimintaansa koskevia tietoja. Tämän tutkielman osalta tilitoimisto käsitellään anonyymina ja tämän tutkimuksen tuloksiin on tuotu raportista tietosuoja-asetuksen noudattamista koskevat tulokset. Yrityksen toimitusjohtaja ja työntekijät arvioivat ja hyväksyivät raportin toukokuussa 2018. Tässä luvussa käsitellään tutkielman johtopäätökset ja niiden pohdinta vertaamalla haastatteluiden tuloksia viitekehykseen. Viitekehyksen merkitys on lähetymistapa tutkimustulosten analysointiin. Lähestymistavalla tarkoitetaan tämän tutkimuksen tulosten vertailua viitekehyksen tuloksiin.

9.1 Yrityksen nykytila

Yrityksen nykytilan selvittämiseen viitekehyksenä käytettiin Tikkinen-Piri ja muut (2017) määrittelemää 12 tietosuoja-asetuksen vaatimusta yrityksen toimintaan. Tikkinen-Piri ja muut (2017) määrittelevät, että yrityksen tulisi säilyttää vain tietoa, jota ilman yritystoiminta ei ole mahdollista. Haastattelujen perusteella työntekijöiden hallussa saattaa olla tietoja, joiden säilyttämiseen heillä ei ole syytä. Tietojen käyttötarpeet on määriteltävä, jotta voidaan arvioida, onko jokin tieto turhaa vai tarpeellista. Haastatteluissa selvisi, että paljon tietoa säilötään varalta, koska sitä voi joskus tarvita. Tämä ei kuitenkaan ole riittävä perustelu sille, että yritystoiminta ei olisi mahdollista ilman niitä. Vanhentuneita tietoja on ryhdytty tuhoamaan, vaikka siihen aiheuttaa haastavuutta lakisääteiset säilytysajat. Vaikuttaa siltä, että yrityksen työntekijät eivät ole täysin tietoisia mikä tieto on turhaa ja mikä ei.

Tietosuoja-asetus (2016/679) vaatii varmistamaan, että tietosuoja-asetusta noudatetaan myös maissa, joiden kanssa yritys on tekemisissä. Haastatteluiden perusteella yrityksellä on asiakkaita vain EU:n sisällä, joten myös näiden asiakkaiden on noudatettava tietosuoja-asetusta. Armbrust ja muut (2010) huomauttavat, että myös pilvipalveluiden tarjoajien on noudatettava tietosuoja-asetusta. Haastatteluiden perusteella yrityksen työntekijät ovat tiedostaneet, että ohjelmistotalon eli ohjelmistopalveluiden ja pilven tarjoajan kanssa on varmistettava tietosuoja-asetuksen noudattaminen heidän palveluissaan.

Sisäänrakennettu tietosuoja tarkoittaa tietosuojaperiaatteiden noudattamista; käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja

luottamuksellisuus, sekä rekisterinpitäjän osoitusvelvollisuus (Talus ja muut, 2017). Haastattelujen perusteella kaikki yrityksen työntekijät pääsevät käsittelemään kaikkea yrityksen hallussa olevaa tietoa. Tietoja käsitellään vain työnteon tai lain vaatimusten nojalla. Haastattelujen mukaan palkanlaskentaa ei pystytä suorittamaan ilman henkilötunnusta ja henkilötietoja, joten työnteko velvoittaa tietojen hankintaa asiakkailta. Näin ollen tietojenkäsittelyn oikeusperustana on asiakassuhteen toteuttaminen, joka on määritelty asiakassopimuksissa. Henkilötietojen pyytämisen perusteena on kirjanpidon ja palkanlaskennan lakisääteisten raporttien tuottaminen. Kuten edellä mainittiin, tietojen minimoinnissa on haasteita ja puutteita. Tietojen säilytyksen rajoittamisessa on myös tehtävää. Vaikuttaa siltä, että kaikki työntekijät pääsevät kaikkeen tietoon käsiksi, vaikka heillä ei ole siihen tarvetta. Ryhmähaastattelussa todettiin, että osalle työntekijöistä on rajattu pääsyoikeuksia. Tietojen saatavuutta on ryhdytty rajoittamaan, mutta osaan arkistoista kaikilla työntekijöillä on pääsyoikeus. Yksilöhaastattelujen perusteella kaikki haastateltavat eivät olleet tietoisia pääsyoikeuksien rajauksista. Tästä voidaan päätellä, etteivät työntekijät ole täysin tietoisia heitä koskevista rajauksista tai käyttöoikeuksista. Sijaistamisen helpottamiseksi asiakkaiden tietoja ei voida kokonaan rajata yhdelle työntekijälle. Henkilötietojen käsittely on perusteltu selkeästi, mutta kirjallinen ja selkeä dokumentaatio puuttuu. Oletusarvoisen tietosuojan noudattamiseen yrityksen on myös dokumentoitava tietojen käyttötarkoitus (Talus ja muut, 2017). Tietoa kerätään, kun asiakkailta tarvitaan lisätietoja kirjanpitoa tai palkanmaksua varten. Tiedot myös käsitellään asiakkaan tarvitsemia toimintoja varten eli kirjanpitoa ja palkanlaskentaa. Tiedon luovuttamisessa ollaan varovaisia ja tietojen siirrosta asiakkaalle tai toiseen tilitoimistoon kerätään asiakkaan kuittaus siirrosta. Arkistoinnissa noudatetaan lakisääteisiä säilytysaikoja. Paperiset tiedot poistetaan silppuriin. Sähköisessä muodossa olevan tiedon poistaminen on haastavaa, koska sähköpostissa pyörii arkistoimatonta tietoa. Sisäänrakennetun tietosuojan noudattamisessa yrityksen suurin puute on osoitusvelvollisuus eli dokumentaatio tietosuojaperiaatteiden noudattamisesta puuttuu kokonaan. Muiden periaatteiden noudattaminen vaikuttaa olevan tiedossa tai hoidettu.

Tikkinen-Piri ja muut (2017) toteavat, että tietosuoja-asetuksen noudattamiseen on suositeltavaa ottaa käyttöön käytännesäännöt. Tällä hetkellä yrityksellä ei ole otettu käyttöön tietosuojakäytäntöjä tai ohjeistusta tietojen käsittelyyn. Haastattelujen perusteella kukaan työntekijöistä ei ollut tietoinen alakohtaisista käytännesäännöistä. Henkilötietojen käsittely perustuu työntekijöiden omiin käytäntöihin ja tapoihin. Joitakin käytäntöjä työntekijät ovat sopineet keskenään ja kahvipöytäkeskusteluista on opittu myös tietosuoja-asetuksesta. Dokumentoidut käytännesäännöt ovat osa osoitusvelvollisuutta. Dokumentoiduilla käytännesäännöillä yritys voi osoittaa noudattavansa tietosuoja-asetusta. (Tikkinen-Piri ja muut, 2017.)

Tietosuoja-asetus (2016/679) vaatii, että tietosuojaloukkaukseen on reagoitava mahdollisuuksien mukaan 72 tunnin kuluessa tapahtuneesta. Haastattelujen mukaan kaikki yrityksen työntekijät reagoivat tietomurtoon tai tietoturvaloukkaukseen erillä tavalla. Kukaan ei vastannut 72 tunnin aikarajaa tai yrityksen ohjeistusta loukkaustilanteeseen. Haastattelujen perusteella tietomurtoa ei ole aiemmin tapahtunut yrityksessä, joten tietämättömyyttä perusteltiin myös sillä. Haastattelujen perusteella yrityksen työntekijöillä ei ole tietoa valvontaviranomaisen kanssa tehtävästä yhteistyöstä tietoturvaloukkauksen sattuessa. Ohjeistus tietomurtoon tai tietoturvaloukkaukseen kannattaa luoda sekä ohjeistaa työntekijöitä tunnistamaan nämä tapahtumat. Vaikutti siltä, etteivät työntekijät uskoneet tietoturvaloukkauksen tapahtumiseen, joten myös ohjeistus puuttui.

Kaikki yrityksen työntekijät tiesivät tietosuoja-asetuksen laiminlyönnistä syntyvät sakot. Tietosuoja-asetuksen (2016/679) mukaan vähäisestä rikkomuksesta aiheutuu vain huomautus. Haastattelujen perusteella tietosuoja-asetuksen noudattamisen vastuu on jaettu yrityksen työntekijöiden kesken, toimitusjohtajalla on suurempi vastuu kuin muilla työntekijöillä. Vaikuttaa siltä, että ainoastaan tietosuoja-asetuksen määräämät sakot saavat työntekijät noudattamaan tietosuoja-asetusta, koska kaikki työntekijät tiesivät tietosuoja-asetuksen laiminlyönnistä aiheutuvat sanktiot. Haastatteluiden perusteella tietosuoja-asetuksen vaatimia asioita ei ole tehty, koska ei ole ollut pakko. Pakolla viitataan siihen, ettei aiemmin ole määrätty sakkoja tai sanktioita tietosuoja-asetuksen vaatimusten laiminlyönnistä. Tämä on ristiriidassa sen kanssa, ettei työntekijöiden mielestä tarvita sanktioita seuraamukseksi vääristä toimintatavoista.

Ryhmähaastattelussa selvisi, ettei yritys aio nimittää tietosuojavastaavaa, koska se ei ole pakollista heille. Tietosuoja-asetuksen (2016/679) mukaan tietosuojavastaavan nimittäminen ei ole pakollista kaikille yrityksille. Tikkinen-Piri ja muut (2017) toteavat artikkelisaan, että tietosuojavastaavan nimittäminen voi olla haastavaa pienelle yritykselle, koska tarvittavaa osaamista ei löydy. Heidän mukaansa tietosuojavastaavan nimittäminen yrityksen sisällä voisi olla hyödyllistä tietosuoja-asetuksen käyttöönoton helpottamiseksi.

Tietosuoja-asetus (2016/679) vaatii yrityksiä informoimaan rekisteröityjä siitä, millaista tietoa heistä kerätään, miten tietoa käsitellään ja suojataan. Yrityksellä on siis oltava tietämys mihin tietoja on säilötty (Tikkinen-Piri ja muut, 2017). Haastatteluissa selvisi, että yrityksen työntekijät yrittäisivät parhaansa mukaan vastata mahdollisiin tietopyyntöihin. Pyyntöön vastaaminen on haastavaa, koska pyyntöjä ei ole tullut aikaisemmin, joten ohjetta ei ole ollut tarvetta luoda. Työntekijöiden täytyisi selvittää missä kaikkialla tietoa sijaitsee ennen kuin sitä voi jakaa asiakkaalle. Haastatteluissa työntekijät totesivat, että asiakkaan tietoahan se heidän säilyttämänsä tieto on, joten se pitäisi voida palauttaa asiakkaalle. Yrityksen työntekijät tunnistivat uusien tietosuoja-asetuksen mukaisten sopimusten luomisen tarpeen ja osa myös tiesi, että taloushallintoliitto on luvannut toimittaa yrityksille uuden sopimuspohjan, joka sisältää tietosuoja-asetuksen vaatimukset suostumukselle. Haastattelujen perusteella asiakkaiden kanssa tullaan tekemään tietosuoja-asetuksen mukaiset sopimukset. Osa tilitoimiston työntekijöistä oletti, että kaikkeen asiakkaan toimittamaan materiaaliin on suostumus. Tietosuoja-asetuksen 28 artiklan mukaan henkilötietojen käsittelijän on noudatettava rekisterinpitäjän ohjeistusta tietojenkäsittelystä, joten tilitoimiston henkilökunnan on oltava tietoisia tietojenkäsittelysopimuksen sisällöstä.

Tietosuoja-asetus sisältää rekisteröidyn oikeuden ”tulla unohdetuksi”, jonka nojalla yrityksen on poistettava henkilöä koskevat tiedot hänen pyytäessään (Tikkinen-Piri ja muut, 2017). Haastateltavat totesivat tiedon poistamisen hankaluuden kirjanpitolain (1336/1997) vuoksi, koska laki velvoittaa säilyttämään kirjanpitoaineistoa 10 vuotta. Tietojen siirtämiseen yrityksessä on toimintatavat ja ohjeet, joiden avulla tiedot voidaan siirtää luotettavasti asiakkaalle tai toiseen yritykseen. Tietojen hakijalta otetaan kuittaus, jolloin yritykselle jää todiste tietojen siirrosta. Haastateltavien vastaukset kuitenkin vaihtelivat ja muutamalla työntekijällä ei ollut ollenkaan tietoa oikeasta tavasta siirtää asiakkaan tietoja. Tietojen poistaminen ja siirtäminen kannattaisi käydä läpi koko henkilöstön kanssa, jotta työntekijät osaavat reagoida oikein mahdollisen tilanteen sattuessa. Tietojen poistamiseen ja siirtämiseen sovittavat toimintatavat olisi myös suositeltavaa kirjata sopimukseen tilitoimiston ja asiakasyrityksen välillä, jotta noudatetaan tietosuoja-asetuksen artiklaa 28 eli henkilötietojen käsittelijänä tilitoimisto käsittelee henkilötietoja vain rekisterinpitäjän ohjeiden mukaan.

Tietosuoja-asetus (2016/679) vaatii yrityksiä dokumentoimaan tietojenkäsittelyä ja suorittamaan tietosuojaa koskevan vaikutustenarvioinnin. Tietosuojaa koskeva vaikutustenarviointi on suoritettava vain, jos tietojenkäsittely aiheuttaa käsittelyn kohteelle korkean riskin (Tikkinen-Piri ja muut, 2017). Haastattelujen perusteella yrityksen työntekijät eivät olleet tietoisia tietosuojaa koskevasta vaikutustenarvioinnista, joten he eivät osanneet arvioida sen vaikutuksia tai tarpeellisuutta. Määritelmä tietosuojaa koskevan vaikutustenarvioinnin tarpeesta jättää vielä tulkinnan varaa, joten yritykset joutuvat arvioimaan omaa toimintaansa tarkasti, onko heillä velvollisuutta toteuttaa tietosuojaa koskevaa vaikutusten arviointia. Henkilötietoja käsitellään lähettämällä tietoja asiakkaille ja vastaanottamalla niitä sähköpostitse. Henkilötiedot tallennetaan pilven arkistoihin tai arkistoidaan paperikopioina. Yrityksen kannattaisi dokumentoida nämä tietojenkäsittelyyn liittyvät toiminnot, jotta voidaan myös paremmin arvioida tietosuojaa koskevan vaikutustenarvioinnin tarvetta.

Taulukkoon kolme on koottu toimeksiantajayrityksen nykytila ja tietosuoja-asetuksen noudattamisen vaatimat toimenpiteet tiivistetysti. Vaatimus -sarakkeeseen on koottu tiivistetysti Tietosuoja-asetuksen (2016/679) tilitoimiston henkilötietojen käsittelyä koskevat vaatimukset ja ohjeet. Sarakkeessa on myös tietosuoja-asetuksen artikla, josta vaatimus on peräisin. Vaatimukset pohjautuvat Tikkinen-Piri ja muut (2017) luomaan 12 vaatimukseen tietosuoja-asetuksen noudattamisesta. Nykytila -sarake on toimeksiantajayrityksen työntekijöiden haastatteluiden (yksilö- ja ryhmähaastatteluiden) perusteella laadittu seloste yrityksen nykytilasta. Toimenpiteet -sarakkeeseen on koottu toimeksiantajayritykselle suositeltavia ohjeita eri lähteistä. Toimeksiantajayritys on tilitoimisto, joten toimenpiteet on kohdistettu kyseiselle alalle.

Taulukko 4. Tietosuoja-asetuksen vaatimukset ja suositeltavat toimenpiteet vaatimusten noudattamiseen.

Vaatimus (Tietosuoja-asetus 2016/679)	**Nykytila (Työntekijöiden haastatteluiden perusteella)**	**Toimenpiteet**
Artikla 5: Henkilötietojen käsittelyä koskevat periaatteet: • lainmukaisuus, kohtuullisuus ja läpinäkyvyys • käyttötarkoitussidonnaisuus • tietojen minimointi • täsmällisyys • säilytyksen rajoittaminen • eheys ja luottamuksellisuus • osoitusvelvollisuus	Henkilötietoja käsitellään lainmukaisesti pelkästään työtehtäviin kuuluviin tarkoituksiin. Tietojen minimoinnissa työntekijät totesivat ongelmia, ylimääräistä tietoa saattaa olla. Säilytysajat pyritään huomioimaan, mutta kaikkien asiakirjojen suhteen ei olla varmoja ohjeistuksesta.	Kuntaliiton verkkokaupasta (2018) löytyy ilmainen opas, johon on koottu taloushallinnon säilytysajat. Taloushallintoliitto suosittelee tietosuoja-asetuskyselymallin mukaisen kyselyn lähettämistä ohjelmistotaloille, jotta varmistutaan ohjelmistotoimittajan tietoturvasta ja tietosuoja-asetuksen teknisten vaatimusten noudattamisesta. Taloushallintoliitto tarjoaa myös dokumenttipohjan osoitusvelvollisuuden noudattamiseen, joka koskee erityisesti palkkahallintoa. (Taloushallintoliitto, 2018)

Artiklat 6 ja 7: Käsittelyn lainmukaisuus ja sopimuksen edellytykset	Asiakkaiden kanssa on tehty asiakassopimukset, mutta tietosuoja-asetuksen mukaisia ei ole vielä	Taloushallintoliitto tarjoaa asiakassopimukset, joihin on varmistettu tietosuoja-asetuksen vaatimukset. (Taloushallintoliitto, 2018).
Artikla 9: Erityisiä henkilötietoryhmiä koskeva käsittely	Ammattiliiton jäsenyyksiä, ulosottotietoja ja sairaslomatodistuksia käsitellään yrityksen toiminnassa.	Taloushallintoliitto tarjoaa asiakassopimukset, joihin on varmistettu tietosuoja-asetuksen vaatimukset. (Taloushallintoliitto, 2018). Fredman (2017), suosittaa arkistoimaan työntekijöiden lääkärintodistukset, ulosottodokumentaation, ammattiyhdistys-jäsenyystiedot ja vastaavat omaan mappiinsa lukkojen taakse tai sähköisessä muodossa hakemistoon.
Artiklat 12,13,24 ja 28: Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten. Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä Rekisterinpitäjän vastuu Henkilötietojenkäsittelijä	Asiakassopimukset on tehty asiakkaiden kanssa. Tietojen antaminen on sovittu suullisesti. Työntekijöiden kanssa on tehty salassapitosopimukset	Taloushallintoliiton mukaan tilitoimiston asiakkaita on ohjattava antamaan ohjeistus henkilötietojen käsittelystä. (Taloushallintoliitto, 2018) Taloushallintoliitto tarjoaa tietosuoja-asetuksen mukaiset asiakassopimukset (Taloushallintoliitto, 2018)
Artikla 12: Oikeus saada vastaus pyyntöihin ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa sekä perustelemaan kieltäytymisensä siinä tapauksessa, että rekisterinpitäjä ei aio noudattaa tällaista pyyntöä.	Asiakkaalle annetaan häntä koskevat tiedot	Asiakkaiden pyyntöihin on varauduttava laadituilla tunnistus- ja tiedonantomenetelmillä (Fredman, 2017). Taloushallintoliitto tarjoaa asiakkaan ohjaamiseen tiedotemallin (Taloushallintoliitto, 2018)

Artiklat 15-21, 77-79 ja 82: Rekisteröidyn oikeudet	Asiakkaalle annetaan pääsy häntä koskeviin tietoihin, jos hänet pystytään tunnistamaan. Työntekijöillä ei ole tarkkaa ohjeistusta tietojen poistamisesta. Tietojen siirtämiseen on ohjeistus, jota noudatetaan.	Asiakkaiden pyyntöihin on varauduttava laadituilla tunnistus- ja tiedonantomenetelmillä (Fredman, 2017). Huomioitava lakisääteiset säilytysajat ja tekninen toteutus eli tietojen poisto eri tietojärjestelmistä (VAHTI, 2016).
Artikla 25: Sisäänrakennettu ja oletusarvoinen tietosuoja	Tietojen minimointi on tiedostettu.	Yrityksen on poistettava tiedot, joiden säilyttämiseen ei ole syytä (Tikkinen-Piri ja muut, 2017). Taloushallintoliiton mallipohjat asiakkaalta pyydettävään tietosuoja-ohjeistukseen ja ohjelmistotalolle lähettävään kyselymalliin ovat suositeltavia sisäänrakennetun ja oletusarvoisen tietosuojan noudattamiseen. (Taloushallintoliitto, 2018)
Artikla 30: Seloste käsittelytoimista eli rekisteriseloste	Yrityksen työntekijöillä ei ollut tietoa termistä	Taloushallintoliitto tarjoaa mallin viranomaiselle annettavasta selosteesta, joka täydennetään tilitoimiston tiedoilla (Taloushallintoliitto, 2018).
Artikla 32: Käsittelyn turvallisuus	Yrityksen työntekijät pyrkivät luomaan fyysistä turvallisuutta ovien lukitsemisella ja piilottamalla henkilötiedot asiakkaiden käydessä toimistossa. Salassapitosopimukset henkilökunnan ja siivoojien kanssa on tehty. Tietoturvan tekninen toteutus on ohjelmistotalolla.	Taloushallintoliitto suosittelee tarjoamansa tietosuoja-asetuskyselymallin mukaisen kyselyn lähettämistä ohjelmistotaloille, jotta varmistutaan ohjelmistotoimittajan tietoturvasta ja tietosuoja-asetuksen teknisten vaatimusten noudattamisesta. (Taloushallintoliitto, 2018) VAHTI-raportti (2016) suosittelee tietosuojan ja tietoturvan varmistamista henkilökunnan koulutuksilla.

Artiklat 33 ja 34: Henkilötietojen tietoturva-loukkauksesta ilmoittaminen valvonta-viranomaiselle Henkilötietojen tietoturva-loukkauksesta ilmoittaminen rekisteröidylle	Kaikilla työntekijöillä on oma tapansa tietoturvaloukkaukseen reagointiin ja siihen ei ole ohjeistusta	Ilmoitusta ei tarvitse tehdä, jos tietojenkäsittelijä pystyy osoittamaan, ettei tietoturvaloukkauksesta aiheudu luonnollisen henkilön oikeuksiin tai vapauksiin kohdistuvaa riskiä. (EU 2016/679.) Valtiovarainministeriön VAHTI-raportissa (1/2016) kehotetaan yritystä luomaan dokumentaatiopohja tietoturvaloukkauksesta ilmoittamiseen asianosaisille. Yrittäjät (2018) tietosuojaoppaan ja VAHTI-raportin mukaan ilmoituksen on sisällettävä tietoturvaloukkauksen: • Selkeä kuvaus tapahtuneesta, • Asianomaiset, • Seuraukset, • Toimenpiteet ja • Mahdollisten haittavaikutusten lieventäminen.
Artikla 35: Tietosuojaa koskeva vaikutustenarviointi	Yrityksen työntekijöillä ei ollut tietoa termistä	Tietosuojaa koskevan vaikutusten arvioinnin tarve on kartoitettava.
Artiklat 37-39: Tietosuojavastaava	Yrityksellä ei ole tietosuojavastaavaa	Tietosuojavastaavan tarve on kartoitettava
Artikla 99: Voimaantulo		Tietosuoja-asetusta aletaan soveltamaan 25.5.2018

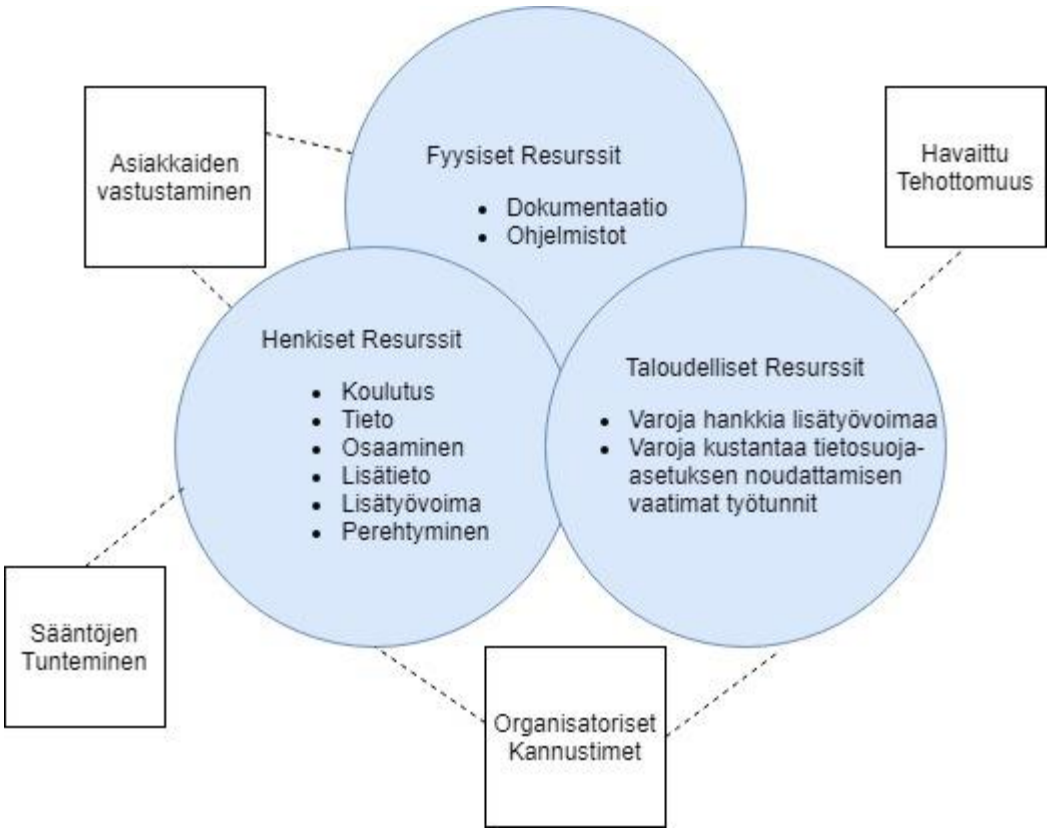
Taulukkoon 4 kerätyt tiedot toimitettiin selvityksineen toimeksiantajayritykselle maaliskuussa 2018. Taulukko oli osa raporttia, joka ohjeistaa yritystä tietosuoja-asetuksen noudattamisessa. Raportissa käsiteltiin yrityksen nimeä ja työntekijöiden nimiä, joten sitä ei tuotu tähän tutkielmaan alkuperäisessä muodossa. Yritys halusi pysyä anonyymina. Taulukko poikkeaa Tikkinen-Piri ja muiden (2017) viitekehyksestä, koska se pohjautuu tietosuoja-asetuksen artiklojen järjestykseen. Toimeksiantajayritykselle toimitettavaa raporttia varten tietosuoja-asetuksesta täytyi huomioida kaikki toimeksiantajayrityksen toimintaan vaikuttavat kohdat.

9.2 Tietosuoja-asetuksen vaikutukset

Tämä kappale vastaa toiseen tutkimuskysymykseen: *”Millaisia muutoksia EU:n uuden tietosuoja-asetuksen noudattaminen luo yrityksen toimintaan?”* Muutokset perustuvat työntekijöiden oletuksiin ennen tietosuoja-asetuksen voimaantuloa.

Toimeksiantajayritys on aineiston keruun aikaan muutosta edeltävässä vaiheessa, joten muutokseen valmistautuminen on vasta aloitettu. (vrt. Ponteva, 2010, s. 25; Luomala 2008). Luomala (2008) esittelee muutoksen suunnitteluun varattavat resurssit; fyysiset olosuhteet, taloudelliset varat, aika, tieto ja osaaminen, ja lisätyövoima. Muutoksen hallintaan vaikuttavia keinoja ovat avoin keskustelu, tuki, tiedotus, osallistuminen, jatkuva muutosviestintä, koulutus ja jatkon hallinta. (Ponteva, 2010, s.37-42; Luomala, 2008.)

Työntekijät listasivat resursseja, joita tarvitaan tietosuoja-asetuksen noudattamiseen ja muutosten käyttöönottoon; koulutusta, sähköisiin järjestelmiin ominaisuuksia tietosuoja-asetuksen noudattamiseen, aikaa, tietoa, osaamista, ohjeistukset, lisätietoa, lisätyövoimaa, alussa seurantaa uusien asioiden noudattamisessa, uudet sopimukset asiakkaiden kanssa, vastuiden jakamista, perehtymistä ja selvittää omaan työhön liittyvät vaikutukset. Haastatteluissa myös ilmeni, että tietosuoja-asetuksen noudattamiseen käytetyt työtunnit lähtevät yrityksen omasta katteesta. Myös lisätyövoima maksaa. Haastatteluissa työntekijät pohtivat myös maksullisia tietosuoja-asetuksen noudattamisen konsultointeja, mutta työntekijät eivät maininneet, että niitä olisi ostettu. Fyysisistä resursseista huomioitiin vain tietosuoja-asetuksen vaatima kirjallinen dokumentaatio. Pilvipalvelut ja ohjelmistojen muutokset hoitaa ohjelmistotalo, jolta palvelut on hankittu. Männistö (2017) huomautti, että myös toimittajien tietosuoja-asetuksen noudattaminen on varmistettava.



Kuva 9. Malli EU:n tietosuoja-asetuksen noudattamisen tekijöistä yhdistettynä yrityksen resursseihin (Mukaillen Gelderman ja muut, 2006; Alhola, 2016, s. 111-117).

Kuvassa 9 on listattu viitekehyksen mukaiset mahdolliset vaikutukset tietosuoja-asetuksen noudattamiseen yhdistettynä tietosuoja-asetuksen vaatimiin resursseihin. Palloihin on kuvattu työntekijöiden havaitsemat resurssit tietosuoja-asetuksen noudattamiseen jotka on kategorisoitu Alholan (2016, s.111-117) määrittelemiin resurssiryhmiin. Katkoviivalla resurssiryhmiin on yhdistetty Gelderman ja muiden (2006) luomat EU:n säännösten noudattamisen toimenpiteet. Haastattelujen perusteella tietosuoja-asetuksen säännöt ja vaatimukset eivät selkeästi olleet selvillä kaikille työntekijöille, joten voidaan sanoa, ettei kukaan ollut täysin varma kuinka tietosuoja-asetusta noudatetaan. Sääntöjen tuntemattomuus selkeästi vaikeuttaa tietosuoja-asetuksen noudattamista yrityksessä. Moni haastateltava myös totesi, että tietosuoja-asetuksen noudattaminen olisi helpompaa selkeillä ohjeilla ja sääntöjen opettamisella. Henkisten resurssien hankkiminen voisi edistää sääntöjen tuntemista ja ymmärtämistä, jolloin tietosuoja-asetuksen noudattaminen olisi mahdollista. Havaittu tehottomuus asetuksen noudattamiseen voidaan havainnoida siinä, että yrityksen työntekijät perustelivat omaa panostamattomuuttaan sillä, että asiakkaat eivät ole valmiita maksamaan lisää palveluista. Osa työntekijöistä totesi, että asiakkaille syntyy kustannuksia asioista, joita eivät ymmärrä tai ole halukkaita ottamaan käyttöön. Taloudellisten resurssien hyödyntäminen lisäisi tehokkuutta asetuksen noudattamisessa, kun työntekijät voisivat käyttää työaikaansa asetukseen valmistautumiseen. Toinen tapa lisätä tehokkuutta olisi ostaa osaavaa lisätyövoimaa hoitamaan tietosuoja-asetuksen vaatimuksia, jolloin muille työntekijöille jäisi aikaa muihin työtehtäviin. Organisatoriset kannustimet toimeksiantajayrityksen toiminnassa ovat johdon tietosuojaosaaminen ja -tietämys, sekä mahdolliset sanktiot. Kuten Gelderman ja muut (2006) toteavat, johdon osaaminen voi toimia kannustimena noudattaa sääntöjä. Haastattelujen perusteella yrityksen johdolta ei ole saatu kirjallista ohjeistusta tietosuoja-asetuksen noudattamiseen. Tästä syystä asetuksen noudattaminen on haastavaa. Yrityksen työntekijät tiedostivat asetuksen noudattamattomuudesta tulevat sanktiot, mutteivat

olleet tietoisia, milloin ja mistä syystä niitä määrätään. Organisatoristen kannustinten lisääminen vaatii taloudellisia ja henkisiä resursseja, koska kannustimia voi olla monelaisia ja yrityksen on valittava niistä itselleen sopivat. Asiakkaiden vastustamista ei ilmennyt haastatteluissa, koska tietosuoja-asetus ei ollut astunut voimaan haastattelujen hetkellä. Tietosuoja-asetus (2016/679) vaatii rekisterinpitäjiä varmistamaan, että henkilötietojen käsittelijä noudattaa tietosuoja-asetusta, joten voidaan olettaa, että asiakas vaihtaa tilitoimistoa, jos tilitoimisto ei noudata tai pysty osoittamaan noudattavansa tietosuoja-asetusta. Näin ollen tilitoimiston on varmistettava henkiset ja fyysiset resurssit ja niiden riittävyys tietosuoja-asetuksen noudattamiseen.

10. Yhteenveto

Tämän tutkimuksen tarkoituksena oli selvittää, miten taloushallinnon alalla toimivan yrityksen pitäisi valmistautua EU:n uuden tietosuoja-asetuksen voimaantuloon 25.5.2018. Tutkimuksen kohteena oli pieni, alle 10 työntekijän kokoinen tilitoimisto. Tutkimuksen kohteena oleva tilitoimisto toimi tämän tutkimuksen toimeksiantajayrityksenä. Haastatteluun osallistuivat kaikki yrityksen yhdeksän työntekijää, joista yksi on myös yrityksen toimitusjohtaja. Tämän tutkimuksen tutkimusmenetelmänä oli laadullinen tapaustutkimus ja aineisto kerättiin työntekijöiden haastatteluilla.

Tutkielman taustalla on toimeksiantajayrityksen luoma toimeksianto. Toimeksianto sisälsi yrityksen nykytilan selvityksen ja ohjeet tietosuoja-asetuksen noudattamiseen, joka vastaa myös tutkimuksen tavoitteeseen. Yrityksen nykytila selvitettiin yrityksen työntekijöiden haastattelujen avulla. Vastauksia verrattiin tietosuoja-asetukseen (2016/679) ja sen asettamiin vaatimuksiin, jolloin saatiin selville muutettavat käytännöt ja tavat. Yhteenvetona yrityksen tehtävälista tietosuoja-asetuksen noudattamiseen eli havaitut puutteet yrityksen nykytilassa verrattuna Tikkinen-Piri ja muiden (2017) 12 vaatimukseen tietosuoja-asetuksen noudattamisesta;

- Luotava käytännöt tiedon säilytykseen, jotta säilytetään vain oikeasti tarpeellinen tieto,
- Henkilökunnan koulutus tietosuojasta ja -turvasta,
- Suojattava henkilötietojen käsittely yrityksen resursseihin nähden sopivalla tavalla,
- Kartoitettava tietosuojavastaavan tarve,
- Uudet tietosuoja-asetuksen mukaiset sopimukset asiakkaiden ja sidosryhmien kanssa,
- Huomioitava asiakkaiden mahdolliset pyynnöt heitä koskevista tiedoista ja luotava käytännöt niihin vastaamiseen,
- Käsittelytoimia koskevan selosteen laatiminen,
- Kartoitettava tietosuojaa koskevan vaikutusten arvioinnin tarve ja
- Kirjallinen dokumentaatio ohjeista ja käytännöistä.

Kirjallisen dokumentaation on sisällettävä ohjeet tietoturvaloukkauksen käsittelemiseen kuvaus tietojenkäsittelyn suojaustoimista, kuvaus ja ohjeet tietojenkäsittelystä (siirtämisestä ja tallentamisesta), arkaluontoisen tiedon erillinen käsittely, käsittelyn oikeusperuste ja tietojen säilytysajat. Yrityksen nykytila tietosuoja-asetuksen vaatimuksiin nähden vaati selkeästi yritykseltä käytäntöjen muuttamista ja uusien asioiden huomioimista. EU:n tietosuoja-asetus vaatii toimeksiantajayritykseltä kirjallista dokumentaatiota henkilötietojen käsittelystä eli tietojenkäsittely on dokumentoitava työntekijöiden ja asiakkaiden ymmärrettävään muotoon. Dokumentaation lisäksi uudet

käytännöt on koulutettava henkilöstölle, jotta varmistetaan koko henkilöstön tietosuojaosaaminen. Haastateltavien näkemykset tietosuoja-asetuksen luomista muutoksista yrityksen toimintaan vaihtelivat haastateltavien välillä. Monet totesivat, että asiakkaita pitää ohjeistaa ja sähköpostin käyttöä mahdollisesti vähentää. Yrityksen työntekijät tarvitsevat aikaa ja tietämystä, jotta voivat noudattaa tietosuoja-asetusta, sekä ohjeistaa mahdollisesti myös asiakkaita sen noudattamisessa.

Tutkielman lisäarvona ja hyötynä muille yrityksille voidaan pitää pienelle taloushallinnon yritykselle selvitettyjä tietosuoja-asetuksen vaatimuksia. Tutkielmassa haastateltiin pienen taloushallinnon yrityksen kaikki työntekijät, joten tutkimus on tarpeeksi kattava kuvaamaan koko toimeksiantajayrityksen toimintaa. Selvitettyjä vaatimuksia ja ehdotettuja ratkaisuja vaatimusten noudattamiseen erilaiset yritykset voivat hyödyntää omaan toimintaansa sopivalla tavalla. Parhaiten vaatimukset soveltuvat pienen tilitoimiston tietosuoja-asetuksen noudattamiseen, koska heille taloushallintoliitto on entuudestaan tuttu. Taloushallintoliitto tarjoaa paljon materiaalia ja tukea tilitoimistoille tietosuoja-asetuksen noudattamiseen. Pienille yrityksille valmiiden käytäntöjen luominen tietosuoja-asetuksen noudattamiseen helpottaisi tietosuoja-asetuksen noudattamista, joten tällä tutkielmalla pyritään myös vastaamaan kyseiseen puutteeseen. Tämän tutkielman tarkoituksena oli myös luoda toimeksiantajayritykselle tietoa tietosuoja-asetuksesta, jotta he pystyvät mahdollisuuksien mukaan neuvomaan omia asiakkaitaan tietosuoja-asetukseen liittyvissä haasteissa.

Aikaisemmasta tutkimuksesta ei löytynyt vastaavaa käytännön ohjeistusta pienille yrityksille tietosuoja-asetuksen noudattamiseen. Vaikka aiempaa tutkimuskirjallisuutta tämän tutkimuksen aiheesta ei löytynyt, opinnäytetöitä aiheesta löytyy paljon. Seuraavat opinnäytetyöt valittiin sillä perusteella, että ne käsittelevät tietosuoja-asetuksen vaatimuksien huomioimista erilaissa yrityksissä.

Korhonen (2018) tutkii opinnäytetyössään tietosuoja-asetusta tilitoimistossa muutosjohtamisen näkökulmasta, joka on hyvin lähellä myös tämän tutkielman aihetta. Korhosen (2018) tutkimuksen tavoitteena on selvittää tietosuoja-asetuksen luomat muutokset kohdeyrityksen toimintaan, sekä selvittää sopiva muutosjohtamisen malli. Tutkimus on laadullinen tapaustutkimus, jonka aineisto on kerätty puolistrukturoidulla haastattelulla. Tutkimustuloksena ovat tietosuoja-asetuksen muutokset tilitoimistolle ja yritykselle sopiva muutosmalli. Erona Korhosen (2018) tutkielmasta tähän tutkielmaan on tutkielman haastatteluiden tavoite. Korhonen (2018) keskittyy kysymyksissään enemmän tietosuoja-asetuksen luomaan muutokseen kuin tietosuoja-asetuksen vaatimuksiin ja niiden kartoittamiseen. Korhosen (2018) tutkielmaan on koottu tietosuoja-asetuksen muutoksia, muttei toimenpiteitä asetuksen noudattamiseen. Korhosen (2018) tutkimuksessa haastateltavat olivat myös enemmän tietoisia tietosuoja-asetuksesta, koska työntekijöitä oli tiedotettu. Tässä tutkimuksessa toimeksiantajayrityksen työntekijöitä ei ollut vielä tiedotettu tietosuoja-asetuksesta, jotta saatiin todellinen kuva yrityksen nykytilasta ennen tietosuoja-asetuksen noudattamista. Osa haastateltavista oli itsenäisesti perehtynyt aiheeseen, joka myös selvitettiin haastatteluissa.

Häkkinen (2017) tutkii opinnäytetyössään tietosuoja-asetusta palkanlaskennan näkökulmasta. Häkkisen tutkielmassa haastateltiin tilitoimiston työntekijöitä tietosuoja-asetuksen vaatimuksista, kuten tässä tutkimuksessa. Häkkisen tutkielman erona tähän tutkielmaan on tietosuoja-asetuksen vaatimusten noudattamiseen luodut ohjeet. Häkkisen tutkielman tavoitteena oli luoda kuvaus tietosuoja-asetuksesta ja selvittää kuinka tietosuoja-asetus vaikuttaa tilitoimistoon.

Paajanen (2017) tutkii tietosuoja-asetuksen vaikutuksia organisaatioihin diplomityössään. Tutkimuksen tavoitteena ovat EU:n tietosuoja-asetuksen vaikutukset organisaatioiden toimintaan ja pilvipalveluiden käyttämiseen. Tutkimusmenetelmänä on puolistrukturoitu haastattelu. Tutkimuksen tuloksena on tarvittavia toimenpiteitä tietosuoja-asetuksen noudattamiseen, sekä Amazon Web Services -pilvipalvelualustan tarjoamat ratkaisut tietosuoja-asetuksen haasteisiin.

Hjerppe (2018) tutkii pro gradu -tutkielmassaan tietosuoja-asetuksen vaikutuksia ohjelmistoarkkitehtuuriin. Tutkimuksen tavoitteena on muuttaa tietosuoja-asetuksen vaatimukset vaatimusmäärittelyksi ohjelmistoarkkitehtuurille. Tutkimusmenetelmänä toteutettiin arkkitehtuuri tapausyritykselle. Tutkimuksen tuloksena syntynyt arkkitehtuuri arvioitiin ja esiteltiin syntynyt arkkitehtuuri. Hjerppe (2016) totesi myös tutkielmassaan, ettei käytänteitä ja malliesimerkkejä tietosuoja-asetuksen noudattamiseen ole vielä.

Jokinen (2019) tutkii maisteritutkielmassaan tietosuoja-asetuksen vaikutuksia henkilötietojen käsittelyyn markkinoinnissa, joka on myös tutkielman tavoitteena. Tutkimusmenetelmänä on lainoppi, joka on oikeustieteellisen tutkimuksen tutkimusmenetelmä. Tutkimuksen tuloksena syntyi selvitys ja ohjeet henkilötietojen käsittelystä markkinointitarkoituksessa.

Edellä mainittujen tutkielmien lisäksi tietosuoja-asetuksen vaikutuksista löytyi useita opinnäytetöitä, jotka käsittelevät tietosuoja-asetuksen vaatimuksia erilaisista näkökulmista. Useat tutkielmat on tehty toimeksiantajayrityksen pyynnöstä, kuten Korhonen (2018) ja Hjerppe (2018) mainitsevat tutkielmissaan. Tämän nojalla yritykset ovat selkeästi ottaneet tietosuoja-asetuksen noudattamisen asiakseen. Edellä mainittujen tutkielmien tutkimustulokset eivät ole vertailukelpoisia tämän tutkielman kanssa, koska niissä ei luoda ohjeistusta tietosuoja-asetuksen noudattamiseen tai luoda kuvausta yrityksen nykytilasta.

Tutkimuksen rajoituksena on haastattelujen ajoitus. Yrityksen työntekijöitä haastateltiin ensin joulukuussa 2017 ryhmähaastattelussa, jonka jälkeen tammi-helmikuussa järjestettiin yksilöhaastattelut. Tietosuoja-asetus tuli voimaan 25.5.2018, joten tietosuoja-asetuksen todellisia vaikutuksia ei ole huomioitu tässä tutkimuksessa. Työntekijät olivat myös perehtyneet eri tavoin tietosuoja-asetukseen, toiset enemmän ja toiset vähemmän. Tutkimus perustuu työntekijöiden oletuksiin haastatteluhetkellä tietosuoja-asetuksen vaatimuksista. Rajoituksena voidaan myös pitää toimeksiantajayritystä. Haastattelujen määrä rajattiin toimeksiantajayrityksen työntekijöihin (9 työntekijää) ja yrityksen toimialaan (taloushallinto).

Tämän tutkimuksen perusteella tulevaisuudessa mahdollisia tutkimuskohteita ovat tietosuojalaki ja alakohtaiset selvitykset tietosuojalain noudattamisesta. Tietosuojalaki (1050/2018) astui voimaan vasta 1.1.2019, joten se rajattiin pois tästä tutkielmasta. Tietosuojalaki korvaa henkilötietolain 1.1.2019 ja sillä täydennetään tietosuoja-asetusta, joten yritysten on myös perehdyttävä tietosuojalakiin ja sen vaatimuksiin. Mahdolliset erot ja lisäykset tietosuoja-asetuksen ja tietosuojalain välillä olisi tärkeä kartoittaa. Aiempaa tutkimusta tutkimalla selvisi, ettei tietosuoja-asetusta ole vielä tutkittu taloushallinnon alalla lähes ollenkaan. Eri aloilla käsitellään erilaista tietoa monin eri tavoin, joten alakohtainen tietosuoja-asetuksen tutkiminen olisi tärkeä tutkimuskohde tulevaisuudessa. Tietosuoja-asetuksen ja tietosuojalain noudattamiseen voisi myös kehittää malleja, joita yritykset pystyisivät hyödyntämään omiin käyttötarkoituksiinsa. Malleilla tarkoitetaan valmiita ohjeita ja suosituksia. Yritykset ovat jo todennäköisesti huomioineet tietosuoja-asetuksen vaatimukset, joten asetuksen ja tietosuojalain

noudattamisen käytäntöjä olisi mahdollista tutkia. Empiirinen tutkimus tietosuoja-asetuksesta on erittäin vähäistä, joten tulevaisuuden tutkimuksia kannattaisi tehdä myös käytännön näkökulmasta.

Lähteet

Alasuutari, P. (2011). *Laadullinen tutkimus 2.0* (4. uud. p.). Tampere: Vastapaino.

Alhola, K. (2016). *Toimintolaskenta* (5. uudistettu painos.). Helsinki: Talentum Media Oy.

Andreasson, A., Koivisto, J., & Ylipartanen, A. (2016). *Tietosuojakäsikirja johdolle* (2. uudistettu laitos (3. painos)). Helsinki: Tietosanoma.

Arkistolaki 23.9.1994/831

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee G, Patterson D, Rabkin A, Stoica I, & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Cvik, E. D., Pelikánová, R. M., & Malý, M. (2018). Selected Issues from the Dark Side of the General Data Protection Regulation. *Review of Economic Perspectives, 18*(4), 387-407.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design-from policy to engineering. *arXiv preprint arXiv:1501.03726*.

De Boer, L., & Telgen, J. (1998). Purchasing practice in Dutch municipalities. *International Journal of Purchasing and Materials Management, 34*(2), 31-37.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review, 32*(2), 179-194.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(02), 92.

Duncan, B., & Zhao, Y. (2018). Risk Management for Cloud Compliance with the EU General Data Protection Regulation. *In 2018 International Conference on High Performance Computing & Simulation (HPCS)* (664-671). IEEE.

Eriksson, P., & Koistinen, K. (2005). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Tampere: Vastapaino.

Fredman, J. (2017). Tietosuoja-asioissa uusia velvoitteita myös pk-yrityksille. *Summa 2017*(3).

Fredman, J. (2018). Henkilötietojen suoja ja kirjanpitolaki - onko vaatimuksissa ristiriita? *Tilisanomat : yritystalouden ja laskennan ammattilehti, 39*(5), 44-47.

Gelderman, C. J., Ghijsen, P. W. T., & Brugman, M. J. (2006). Public procurement and EU tendering directives–explaining non-compliance. *International Journal of Public Sector Management, 19*(7), 702-714.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(2), 279-288.

Hallituksen esitys HE 9/2018 vp: Hallituksen esitys eduskunnalle EU:n yleistä tietosuojaasetusta täydentäväksi lainsäädännöksi.

Harrell, M. C., & Bradley, M. A. (2009). *Data collection methods. Semi-structured interviews and focus groups.* Rand National Defense Research Inst santa monica ca.

Henkilötietolaki 22.4.1999/523.

Hjerppe, K. (2018). Yleinen tietosuoja-asetus ja ohjelmistoarkkitehtuuri. Pro Gradu – tutkielma. Tietojenkäsittelytiede. Turku: Turun Yliopisto

Hoepman, J. H. (2014). Privacy design strategies. In *IFIP International Information Security Conference*, 446-459.

Häkkinen, J. (2017). Tietosuoja työsuhdetietojen ja palkanlaskennan näkökulmasta. Opinnäytetyö. Liiketalouden koulutusohjelma. Satakunnan ammattikorkeakoulu

Jackson, O. (2018). Many small firms are still unprepared for GDPR. *International Financial Law Review.*

Jokinen, S. (2019). EU: N YLEINEN TIETOSUOJA-ASETUS: MITEN ASETUS VAIKUTTAA HENKILÖTIETOJEN KÄSITTELYYN MARKKINOINNISSA. Maisteritutkielma. Oikeustieteiden tiedekunta. Lapin Yliopisto.

Järvinen, P. (2002). *Tietoturva & yksityisyys*. Docendo.

Kirjanpitolaki 30.12.1997/1336.

Korhonen, S. (2018). Muutosjohtaminen: Case Euroopan Unionin uusi tietosuoja-asetus tilitoimistossa. Opinnäytetyö. Liiketalouden koulutusohjelma. Satakunnan ammattikorkeakoulu

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security, 2017*(6), 5-8.

Kuntaliiton verkkokauppa. Lainattu: 1.8.2018, saatavilla: http://shop.kunnat.net/product_details.php?p=326

Kuntatyönantajat 2005. Etätyöstä sovittaessa huomioon otettavaa. Lainattu 15.1.2019, saatavilla: https://www.kt.fi/sites/default/files/media/document/2005-28-liite2.pdf

Käpylä, J. & Salonius, H. (2013). *Tietojohtajan taskukirja: Tietojohtamisen näkökulmia aluekehittämiseen.* [Tampere]: Tampereen teknillinen yliopisto, tietojohtamisen tutkimuskeskus Novi.

Lahti, S., & Salminen, T. (2014). *Digitaalinen taloushallinto*. Helsinki: Sanoma Pro Oy.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Luomala, A. (2008). Muutosjohtamisen abc. *Ajatuksia muutoksen johtamisesta ja ihmisten johtamisesta muutoksessa. Ihmisten ja työhyvinvoinnin johtamisen tutkimus-ja kehittämisryhmä HYWIN. Tutkimus-ja koulutuskeskus Synergos. Tampereen yliopiston kauppakorkeakoulu.*

Mwelu, N., Davis, P. R., Ke, Y., & Watundu, S. (2018). Compliance within a regulatory framework in implementing public road construction projects. *Construction Economics and Building, 18*(4).

Männistö, E. (2017). Miten palkkahallinnossa tulee valmistautua tietosuoja-asetukseen. *Tilisanomat, 6*(2017), 20-21.

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems, 23*(2), 126-150.

Othman, A. E. A., & Suleiman, W. (2013). An analysis of causes of poor attitude to work. *Procedia-Social and Behavioral Sciences*, *97*, 194-200.

Paajanen, E. (2017). Tietosuoja-asetuksen vaikutukset organisaatioihin ja Amazon Web Services–pilvipalvelualustan tuoman hyödyt. Diplomityö. Tuotantotalouden Tiedekunta. Lappeenranta: LUT-yliopisto

Ponteva, K. (2010). *Onnistu muutoksessa*. Helsinki: WSOYpro.

Priyadharshini, G., & Shyamala, K. (2018). Strategy and Solution to comply with GDPR: Guideline to comply major articles and save penalty from non-compliance. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference*. 190-195. IEEE.

Rohunen, A. and Markkula, J. (2017). Development of Personal Information Privacy Concerns Evaluation. Mehdi Khosrow-Pour (ed.). Encyclopedia of Information Science and Technology, Fourth edition. Hershey, PA, Information Science Reference, pp. 4862-4871.

Saario, K. (2018). Taloustiedot, liikesalaisuudet ja tietoturva. *Tilisanomat : yritystalouden ja laskennan ammattilehti, 39*(3), 28-31.

Saario, K., & Vesterinen, P. (2017). Yritysten rikosturvallisuus 2017: Riskit ja niiden hallinta. *Helsinki: Keskuskauppakamari*.

Sarajärvi, A., & Tuomi, J. (2017). *Laadullinen tutkimus ja sisällönanalyysi*. Uudistettu laitos. Tammi.

Sirur, S., Nurse, J. R., & Webb, H. (2018). Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*. 88-95. ACM.

Suomen Kuntaliitto. Kunnallisten asiakirjojen säilytysajat. Määräykset ja suositukset. 2. Taloushallinto. Helsinki 2009.

Suomen perustuslaki 11.6.1999/731.

Suomen Yrittäjät. (2018). Yrittäjyys Suomessa. Lainattu 7.2.2018, saatavilla: https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Sydekum, R. (2018). Can consumers bank on financial services being secure with GDPR? *Computer Fraud & Security, 2018*(6), 11-13.

Syvänen, S. (2003). Työn paineet ja puuttumattomuuden kustannukset. Tutkimus sisäisen tehottomuuden lähteistä ja vaikutuksista. Esimerkkikohteena kuntien sosiaalitoimen vanhuspalveluja tuottavat työyhteisöt. Tampere University Press.

Taloushallintoliitto. (2018). Lainattu 6.5.2018, saatavilla: https://taloushallintoliitto.fi/laatu-tyokalut/tal-laatutyokalut-ja-ohjeet-tilitoimistolle/tietosuoja-tilitoimistossa

Talus, A., Autio, E., Hänninen, A., Pihamaa, H. T., & Kantonen, S. (2017). Miten valmistautua EU: n tietosuoja-asetukseen?. Lainattu 6.2.2018, saatavilla: https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/8c5b9a96-a8ce-4c91-ad06-6e36130bd0e5/Miten+valmistautua+tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimisto. (2018). Lainattu 28.8.2018, saatavilla: http://www.tietosuoja.fi/

Tietosuoja-asetus 27.4.2016/679.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153.

VAHTI 3/2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Valtiovarainministeriö.

VAHTI 2/2011. Johdon tietoturvaopas. Valtiovarainministeriö.

VAHTI 1/2016. EU-tietosuojan kokonaisuudistus. Valtiovarainministeriö.

Varanka, P., Mäkikangas, P., Hyypiä, M., Jalonen, S., & Samppala, A. (2017). Digitalous. *Opas sähköisen taloushallinnon käyttöönottajille. Turku: Turun ammattikorkeakoulu.*

Wright, D., & De Hert, P. (2012). Introduction to privacy impact assessment. In *Privacy Impact Assessment*. 3-32. Springer, Dordrecht.

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, 2017(6), 8-11.

Liite 1: Ryhmähaastattelun kysymykset

Taustatiedot:

- Mikä on työnkuvasi/ammatti?
  - Erittele työtehtäviäsi.
- Mikä koulutustausta sinulla on?

- Kuinka kauan olet ollut töissä tällä alalla?
  - entä tässä yrityksessä?
- Millaisia asiakkaita teillä on?
  - esim. toimialat, yritysmuoto
- Mitä yhteistyökumppaneita teillä on?
  - oletteko ulkoistanut palveluita, mitä?

Koulutus ja tietämys:

- Miten ymmärrät tietosuojan ja (tietoturvan)?
  - Miten ne eroavat?
- Miten huomioit tietosuojan työssäsi?
- Onko henkilöstöä koulutettu tietosuoja asioihin?
  - Miten?
  - Mistä muualta he ovat saaneet tietoa?
  - Onko teillä tietosuoja ohjeistusta yrityksen sisällä?
  - Onko työntekijöillä salassapito-sopimuksia?
- Mitä tiedätte uudesta tietosuoja-asetuksesta?
  - Mitä muutoksia tietosuoja-asetus mielestäsi luo työhösi?

Yhteenveto, tuliko kaikki sanottua onko vielä mielessä?

Tietojenkäsittely:

- Mitä tietoa teillä käsitellään, luetelkaa mahdollisimman paljon, lista?
  - Mihin tietoa käytetään?
  - Miten tietoa käsitellään?
  - Keiden tietoja käsittelette?
  - Mikä käsittelemästänne tiedosta teidän mielestänne on arkaluontoista?
    - millä perusteella?
  - Käsitelläänkö arkaluontoista tietoa erillä tavalla kuin muuta tietoa?
  - mihin arkaluontoista käytetään?
- Tietävätkö asiakkaanne miten heidän tietojaan käsitellään?
  - Ovatko he antaneet suostumuksensa tietojen käsittelyyn?
  - Millaisessa muodossa suostumukset ovat?
  - Onko asiakkaalla mahdollisuus poistaa häntä koskevat tiedot?
    - Jos on, miten se toteutetaan?
  - Onko asiakkaalla mahdollisuus poistaa häntä koskevat tiedot?
    - Jos on, miten se toteutetaan?

    - Millä tavoin asiakkaat tunnistetaan (esim., Katso-tunnistus tai TUPAS-tunnistus)?
- Onko teillä asiakkaita Euroopan unionin ulkopuolella tai muita?
    - Jos on, missä maissa?

Yhteenveto, tuliko kaikki sanottua onko vielä mielessä?

Valvonta ja ohjeet:

- Miten tietoa säilytetään teillä?
    - Säilytetäänkö arkaluontoista tietoa eri tavalla kuin muuta?
- Valvotaanko tiedon käsittelyä ja säilytystä mitenkään organisaation sisällä esim. esimiehen toimesta?
- Valvotaanko tiedon käsittelyä ja säilytystä mitenkään organisaation ulkopuolelta esim. auditoinneilla?
- Onko teillä dokumentaatiota tietojenkäsittelystä (esim., asiakkaiden tietojen keräämisestä ja varastoimisesta)?
    - Jos on, millaisia?
- Onko teillä toimintaohjeita tietomurron käsittelyyn?
    - Jos tietomurto tapahtuu, miten reagoisit siihen?
- Onko teillä organisaation sisällä käytössä sanktioita tai seuraamuksia, siitä että ohjeita ei noudateta?
    - Jos on, millaisia?
    - Millainen toiminta on mielestäsi rangaistavaa?
- Onko teillä nimettynä tietosuojavastaavaa?
- Onko teillä toteutettu tietosuojaa koskeva vaikutusten arviointi?
    - Mikä on tarkoituksenne kerätä tietoja?

Haasteet

- Millaisia haasteita tietosuoja luo työhönne?
    - miksi?
- Mikä tuntuu haastavalta?
- Onko organisaatiossanne tulossa muutoksia, kuten tietojärjestelmän hankinta?
- Onko nyt lopuksi herännyt kysymyksiä ja tavoitteita työlle?

Liite 2: Yksilöhaastattelun kysymykset

Tausta:

- Mikä on ammattisi/ työnkuvasi?

Tietovirrat:

- Mitä tietovirrat mielestäsi ovat?
- Mitä henkilötietoja käsittelet työssäsi?
- Mitä tietoa lähetät asiakkaille?
- Lähetätkö tietoa muille kuin asiakkaille?
    - Millaista ja kenelle?
- Mitä tietoja saat asiakkailta?
- Millä tavoin tietoja lähetetään tai saadaan?
- Näetkö riskejä tietojen lähettämisessä tai saannissa?
    - Millaisia?

Tietovarannot:

- Mitä tietovarannot mielestäsi ovat?
- Mitä tietovarantoja sinulla on käytössä, esimerkiksi henkilörekisterejä?
- Miksi keräätte ja säilytätte henkilötietoja, eli miten perustelet tietojen säilytyksen ja keräämisen?
- Missä henkilötietoa säilytetään?
- Näetkö riskejä tietojen säilytyksessä?
    - Millaisia?

Tietosuoja:

- Millaisia vaikutuksia tietosuojalla ja sen noudattamisella on työhönne?
- Millaisia keinoja sinulla on tietovirtojen ja tietovarantojen suojaamiseen?
    - Millaisia hallinnollisia keinoja?
    - Millaisia teknisiä keinoja?
    - Miten tietojen käyttöä valvotaan ja rajoitetaan?

Tietosuoja-asetus:

1. Onko sinulla hallussa henkilötietoja, joita et enää tarvitse tai sen säilyttämiseen syytä?
    - Tiedätkö miten näitä tietoja pitää käsitellä?
2. Missä maissa sinulla on asiakkaita?
3. Oletko tietoinen yrityksen tietosuoja käytännöistä?
    - Jos olet, miten noudatat niitä työssäsi?
4. Onko teidän alallanne alakohtaisia käytännesääntöjä tietosuoja-asetuksen noudattamiseen?

   - Jos on, millaisia?
5. Mikä on mielestäsi tietomurto tai tietoturvaloukkaus?
   - Miten reagoit sellaisen sattuessa?
6. Tiedätkö mitä seuraa uuden tietosuoja-asetuksen laiminlyönnistä?
7. Kuinka reagoit asiakkaan pyyntöön saada häntä koskevat tiedot haltuunsa?
8. Ovatko asiakkaat antaneet suostumuksensa tietojensa käsittelyyn?
   - Millaisen?
9. Miten hoidat asiakkaan pyynnön poistaa häntä koskevat tiedot?
10. Miten hoidat asiakkaan pyynnön siirtää häntä koskevat tiedot?
11. Tiedätkö mitä tietosuojaa koskeva vaikutustenarviointi tarkoittaa?
12. Tiedätkö mitä tarkoittaa rekisteriseloste tai tietosuojaseloste?

Muutos:

- Millaisia vaikutuksia uudella tietosuoja-asetuksella ja sen luomilla muutoksilla on työhösi?
- Millaisia vaikutuksia uudella tietosuoja-asetuksella on koko yrityksen toimintaan?
- Mitä sinun mielestäsi yritys tarvitsee uuden tietosuoja-asetuksen noudattamiseen? esim. fyysiset olosuhteet, taloudelliset varat, aikaa, tietoa ja osaamista, lisätyövoimaa.
- Mistä olet saanut tietoa uuden tietosuoja-asetuksen vaikutuksista?